ST+STE



LE PACK ANTI VIRUS

Une solution radicale pour la protection de vos programmes.

EDITIONS MICRO APPLICATION



Üwe GOHLKE

Le Pack ANTI VIRUS

Editions MICRO APPLICATION

MICRO APPLICATION
58, Rue du Faubourg Poissonnière
75010 PARIS

ISBN : 2-86899-216-1

Auteur : Üwe Gohlke
Traduction française assurée par Roxane Zgripcea

Collection dirigée par Mr Philippe OLIVIER
Edition réalisée par Frédérique BEAUDONNET

Remarques importantes

❒ Erreurs de programmes

Aucun programme n'est à l'heure actuelle en mesure de fonctionner sans erreur. Nous ne prétendons pas échapper à cette réalité et de ce fait, nous ne pouvons pas garantir un fonctionnement sans erreur de notre programme sur votre installation. Cette lacune est principalement due à l'extrême diversité des configurations matérielles réalisables, qu'il nous est impossible de couvrir intégralement dans nos tests. Ce n'est qu'après avoir rencontré des problèmes sur une configuration particulière que nous pouvons effectuer les tests appropriés pour mieux adapter notre programme et en assurer un fonctionnement optimal sur la configuration testée. Nous déclinons bien entendu toute responsabilité pour les erreurs qui surviennent indépendamment de la configuration.

❒ Actualités

Nous recevons parfois des modifications de dernière minute à l'heure où le guide d'utilisation se trouve déjà en impression, trop tard donc pour en tenir compte dans le manuel. Dans certains cas, il s'avère nécessaire, pour des raisons liées à la maintenance du produit, de modifier une partie du programme, sans qu'il soit possible d'en rendre compte dans le manuel.

Tous ces incidents de parcours nous ont amenés à chercher un moyen de communiquer aux utilisateurs les informations de dernière heure ; nous avons donc décidé d'inclure dans la disquette programme un fichier appelé "Lisezmoi" avec toutes les informations complémentaires qui, pour diverses raisons, n'ont pas pu être intégrées dans le livre lui-même. Il est bien évident que ce fichier ne figurera sur votre disquette qu'en cas de besoin. Avant de lancer le programme pour la première fois, vérifiez si votre disquette contient ce fichier d'information.

Vous pouvez consulter le fichier "Lisezmoi" sans grand effort, directement à l'écran. Cliquez deux fois sur le bouton gauche de la souris. La fenêtre de dialogue qui s'affiche sur votre écran vous propose le choix entre une lecture directe et une sortie sur l'imprimante. Si vous optez pour une consultation directe, cliquez sur la case VISUALISER. Si toutefois vous voulez le sortir sur votre imprimante, cliquez sur la case IMPRIMER.

❒ Un dernier conseil ....

Si vous désirez nous écrire, n'oubliez surtout pas d'indiquer votre configuration. C'est pour nous le seul moyen de vous apporter une aide précise et efficace.

Préface

Cet ouvrage, accompagné du programme VIRtuel, est né d'un profond désir d'offrir au public un moyen de protection complet et efficace contre tous les virus informatiques présents et à venir sur ATARI ST, et de lui apporter toutes les informations complémentaires sur les virus les plus récents.

Les anti-virus dont nous disposions tout au début du développement des systèmes Atari ST étaient insuffisants car ils s'attaquaient uniquement aux virus les plus connus et négligeaient parfois certains aspects d'ordre matériel. Ainsi, certains antivirus se sont avérés incapables d'examiner le disque dur, d'autres en revanche ne parvenaient pas à convaincre sur le plan de la convivialité ; la plupart d'entre eux ne possédaient pas la faculté de s'adapter aux besoins spécifiques en matière de sécurité, et enfin, ils n'offraient pas aux utilisateurs la possibilité de les adapter aux nouveaux virus.

Dans les deux derniers cas, l'utilisateur restait tributaire des mises à jour effectuées par le concepteur lui-même. Le développement de tout nouveau produit dans ce domaine doit s'appuyer sur les expériences précédentes pour tenter d'une part de combler les lacunes existantes, et d'autre part, de développer et consolider les aspects qui se sont révélés positifs.

L'hystérie qui s'est emparée des utilisateurs de micro-ordinateurs familiaux et professionnels à la fin de l'année 1987 et jusqu'au milieu de l'année 1988 autour de l'apparition de plus en plus fréquente de virus informatiques sur ce type de systèmes, s'est quelque peu apaisée mais le danger qui émane des virus n'en est pas moins vivant et ne devrait pas tomber dans l'oubli.

L'idée qui a donné naissance à ce logiciel de protection sur Atari ST était de mettre au point un produit efficace qui rappelerait d'une part les dangers potentiels, en s'appuyant notamment sur un certain nombre de cas d'infections parmi les plus récents, et qui proposerait d'autre part des mesures de protection concrètes, ainsi qu'une aide pratique en cas d'infection sur un Atari ST, sans

toutefois raviver le mouvement de panique. Bien au contraire, l'objectif de cet ouvrage est de sensibiliser les utilisateurs face à ce fléau, car seul celui qui connaît le danger saura se protéger efficacement.

Dans cette optique, cet ouvrage lance un appel à tous les programmeurs qui se trouvent confrontés aux virus informatiques : pensez aux dangers qui émanent de votre activité et n'oubliez pas que toute nouvelle connaissance et tout nouveau développement auxquels vous contribuez peut servir des causes beaucoup moins nobles entre les mains d'individus mal intentionnés, même s'ils ne sont pas eux-mêmes capables d'accomplir de tels exploits. Et comme personne n'est infaillible, vous ne maîtrisez pas totalement les conséquences de vos découvertes.

La recherche dans le domaine des virus informatiques est sans nul doute constructive et nécessaire, les découvertes d'aujourd'hui donneront peut-être un jour naissance à une nouvelle génération de systèmes d'exploitation "vivants", capables de penser et de se développer eux-mêmes. De ce point de vue, toute expérience arbitraire ayant pour objet la manipulation de virus sur un sujet vivant, qui n'est autre que l'utilisateur profane, constitue, sans son consentement du moins, un acte criminel. De ce fait, tous ceux qui participent de près ou de loin à ce genre de tests comprendront sans doute que, dans l'intérêt général, ils devront être considérés comme des criminels en puissance. Changer le monde à la façon d'un Frankenstein, ce n'est certainement pas ce que vous recherchez.

Les connaissances que vous possédez devront être mises en pratique de façon constructive et en étroite collaboration avec d'autres spécialistes dans ce domaine. La publication d'un ouvrage comme celui-ci, même s'il a été réalisé dans l'unique but d'offrir au public un moyen de protection optimal contre les virus, livre d'une façon ou d'une autre un certain nombre d'informations sensibles auxquelles nous avons fait allusion dans les pages précédentes. Cet ouvrage éveillera sans doute chez certains lecteurs un vif intérêt pour les virus informatiques et peut-être leur donnera-t-il même l'idée d'en programmer eux-mêmes. D'autres lecteurs en revanche commenceront peut-être à s'inquiéter pour de bon.

Quoi qu'il en soit, l'auteur de ce livre suppose chez le lecteur un certain degré de responsabilité et espère que les programmeurs prendront à coeur l'appel qui leur a été adressé. Mais si la crainte

s'empare de vous, sachez qu'il y a une solution à tout problème ; on peut très bien se protéger contre les virus informatiques, à condition de prendre certaines précautions.

Certains penseront peut-être : "et en plus il veulent faire de l'argent avec la peur et l'ignorance du public" ou bien "on propage d'abord un virus et puis on cherche à tirer profit de son antidote". Pendant la préparation de cette ouvrage, il m'a été donné d'entendre toutes sortes de réflexions.

Pour répondre à toutes ces objections, je ne peux que dire ceci : Je n'ai développé ni propagé aucun virus, j'ai créé le programme VIRtuel dans l'unique but de me protéger moi-même. On ne peut tout de même pas me reprocher de gagner ma vie, entre autres, avec le développement d'un tel produit - le garagiste répare bien les dégâts causés par autrui et que le propriétaire ne peut pas réparer lui-même.

Les ouvrages et les périodiques spécialisés qui m'ont aidé à écrire ce livre, ainsi que les témoignages de certains utilisateurs sur ce thème, ne font pas le tour de la question ; ils se contentent d'aborder certains aspects isolés qui ne mettent pas en lumière toute l'étendue du problème soulevé par les virus qui sévissent actuellement sur les systèmes informatiques.

La plupart des sinistres provoqués par des virus n'ont vraisemblablement jamais été rendus publics, car l'annonce d'un tel incident ne ferait qu'aggraver les préjudices subis par leurs victimes. Quel est celui qui serait prêt à avouer publiquement ses lacunes en matière de sécurité, tout en sachant qu'une mauvaise publicité ne ferait que nuire à sa réputation. Par conséquent, le bilan est vraisemblablement très lourd mais les chiffres réels restent encore dans l'ombre.

❐ Comment aborder ce livre ?

Il propose un aperçu global des virus informatiques, en particulier ceux qui touchent les systèmes Atari ST, analyse les dangers qui en découlent puis décrit le moyen de lutte, le programme VIRtuel.

❐ **Voici un bref aperçu de son contenu :**

➠ Chapitres 2, 3 :

Nous allons vous présenter ici quelques exemples d'épidémies rendues publiques ces dernières années avec leurs conséquences et nous décrirons les principes de l'action des virus et en particulier des virus spécifiques au système Atari ST. Même les utilisateurs les plus chevronnés y trouveront sans doute une aide précieuse.

➠ Chapitres 4, 5 :

Ils décrivent le fonctionnement du programme VIRtuel sur Atari ST, qui est fourni avec ce livre. Ils s'adressent à tous ceux qui désirent le mettre en oeuvre comme un outil de protection contre les virus sur Atari ST. Vous y trouverez une description détaillée des fonctions du programme et apprendrez comment utiliser VIRtuel avec un maximum d'efficacité. Plus tard, lorsque vous serez familiarisés avec la manipulation du programme, ce chapitre pourra également vous servir de référence, en cas d'infection. Avant de lancer le programme VIRtuel, lisez attentivement ces chapitres. Ensuite, allumez votre Atari ST et relisez-les une seconde fois, en exécutant pas à pas les instructions fournies. Dans certaines sections vous trouverez des renvois à d'autres chapitres pour vous guider dans vos recherches. Mais ne vous précipitez pas tout de suite dans les détails ; ces renvois vous aideront tout simplement à trouver au plus vite les informations recherchées au cas où vous utiliseriez ce livre comme un ouvrage de référence.

➠ Chapitre 6 :

Il est écrit par Maître Alain BLOCH, Avocat à la cour d'appel de Paris. Il nous expose tout ce qu'il faut savoir sur le Droit français en matière de protection contre ce nouveau fléau informatique.

Sommaire

1. Introduction 15

1.1. Les dangers 18

1.2. Conséquences 22

1.3. Historique 23

1.4. Définition des virus 32

2. Les différentes catégories de virus 37

2.1. Boot-virus 39

2.2. Link-virus 39

2.2.1. Virus écrivant par dessus les programmes 40

2.2.2. Link-virus n'écrivant pas par dessus les programmes 42

2.3. Virus résidents en mémoire 44

2.4. Virus évolutifs 46

2.5. Virus batch 46

2.6. Bactéries 47

2.7. Chevaux de Troie 47

2.8. Vers 48

3. Les virus Atari 51

3.1. Les virus du boot-secteur 53

3.2. Les link-virus 56

3.2.1. Le "bacille du charbon" 56

3.2.2. Le virus VCS 57

4. Le programme VIRtuel 59

4.1. Conditions requises 59

4.2. Connaissances préalables 59

4.3. Fonctionnement du programme VIRtuel 60

4.4. Installation de VIRtuel 62

4.4.1. T1.prg 62

4.4.2. T2.acc 63

4.5. Le travail avec VIRtuel 64

4.5.1. Le menu et l'écran 64

4.5.2. Vérification manuelle 69

4.5.2.1. Le dépistage des boot-virus 70
4.5.2.2. Le dépistage des link-virus 76
4.5.2.3. Etablir un diagnostic 80
4.5.2.4. Messages d'avertissement 87

4.5.3. Vérification automatique ("Petit" Diagnostic) 90

4.5.3.1. Constituer une liste de logiciels 91
4.5.3.2. Modification de la liste de logiciels 97
4.5.3.3. Définir un intervalle de temps entre deux vérifications . 102
4.5.3.4. Messages d'avertissement 103

4.5.4. Archiver les boot-secteurs 109

4.6. Messages d'erreurs 114

4.7. Format des fichiers de résultats 116

5. Que faire en cas d'infection ? 119

5.1. Critères d'infection 119

5.2. Mieux vaut prévenir que guérir 121

5.2.1. Où sont les dangers ? 121

5.2.2.1. Dix règles d'or 122

5.3. Décontamination 123

5.3.1.Boot-virus 123

5.3.2. Link-virus 126
5.4. Outils de diagnostic 126
5.4.1. Le contrôleur de disquette 127
5.4.2. Désassembleur 127
5.4.3. Programmes antivirus 127
6. L'évolution du droit positif français 129
6.1. La nécessité de disposer de moyens de lutte légaux 129
6.2. La généralisation de l'informatique et le sentiment de vulnérabilité qu'elle provoque 129
6.3. L'apparition de la criminalité informatique 130
6.4. Typologie des actes frauduleux 131
6.5. Typologie des délinquants 133
6.6. Coût des sinistres 134
6.7. La problématique juridique 135
6.8. L'insuffisance du droit pénal traditionnel 137
6.9. La proposition de loi Godfrain 145
6.10. L'élargissement des incriminations existantes 146
Annexe 149
Index 155

Chapitre 1

Introduction

L'avènement de l'ordinateur remonte à plus de 20 ans et constitue à l'heure actuelle un élément indispensable dans tous les domaines d'activité. Ils aident à piloter des avions et des voitures, exécutent des simulations complexes, surveillent les opérations médicales dans les hôpitaux, ils ont révolutionné les moyens de communication et, plus récemment, ils se sont même installés dans les foyers. Mais depuis quelque temps, ils présentent des symptômes bien étranges.

Ceux qui côtoient de près ou de loin les ordinateurs en connaissent déjà la cause ; ils savent que cette maladie étrange est l'oeuvre des virus logiciels, une série de miniprogrammes qui se reproduisent tous seuls. Ces virus se propagent avec beaucoup d'astuce d'un ordinateur à un autre et finissent un jour par mettre leurs menaces à exécution, qui sont le plus souvent destructrices. Les dégâts provoqués par l'action des virus mis en circulation par des programmeurs sans scrupules ne sont pas des moindres.

Les virus informatiques se transmettent dans une large mesure par l'échange de logiciels et de données entre utilisateurs et voyagent librement à travers les voies de communications offertes par les réseaux et les boîtes aux lettres. Il est bien évident que l'homme ne contractera aucune maladie au contact d'une disquette infectée mais il risque de subir des pertes considérables lorsqu'il introduit la disquette infectée dans son lecteur et lance les programmes qu'elle contient. C'est à partir de ce moment que l'épidémie se

déclenche réellement. Le virus se reproduit et contamine progressivement tous les autres programmes.

Une fois lancé, le programme infecté transmet le virus à d'autres programmes. Tout comme leurs congénères biologiques, les virus informatiques nécessitent la présence d'un hôte. De façon générale, le virus informatique se compose d'une empreinte virale et d'un noyau, et porte en lui une fonction de manipulation. Une fois qu'il a pénétré dans l'ordinateur, l'intrus recherche par l'intermédiaire du système de commande central, les programmes stockés dans la mémoire (y compris la mémoire de masse) qui ne portent pas l'empreinte virale caractéristique. A partir de ce moment, le virus se reproduit à chaque fois que l'utilisateur ou le système lance un programme infecté.

Dans certains cas, les virus sont extrêmement difficiles à repérer, car ils peuvent être définis sous la forme de programmes hibernants, qui somnolent pendant de longues années à l'intérieur de l'ordinateur sans se faire remarquer ; dans d'autres cas, les virus sont astucieusement masqués, de façon à dissimuler leur origine, ou ils peuvent disparaître du programme-hôte au bout de quelques générations. Les chemins empruntés par les virus pour se propager au coeur des programmes sont tout aussi complexes que les chemins utilisés par les données elles-mêmes.

Une fois qu'ils ont pénétré dans le système, les virus s'approprient tous les droits d'accès dont disposent les utilisateurs. Le nombre de .programmes infectés dépend essentiellement des privilèges d'accès attribués aux utilisateurs. Les zones de mémoire communes à l'ensemble d'un réseau permettent aux virus d'atteindre tous les autres systèmes autonomes présents sur le réseau. Pour se glisser à l'intérieur d'un système, les virus peuvent utiliser toutes les interfaces d'entrée.

Une console système mal surveillée ou un canal de télémaintenance offrent autant de possibilités inespérées à un programmeur pour entrer le code de son virus. Parfois, c'est notre curiosité naturelle qui ouvre la porte aux intrus. L'utilisateur qui résiste à la tentation de voir fonctionner un programme dont on lui a vanté les mérites, n'est pas encore né.

Le savoir-faire nécessaire pour programmer un virus n'est plus un terrain réservé aux spécialistes, surtout depuis que la presse informatique s'est aventurée à publier les listings d'un certain nombre de virus et l'on voit à l'heure actuelle des programmeurs relativement peu expérimentés exercer leurs talents sur ce terrain. Les petits bricoleurs de virus ouest-allemands ont déjà acquis la réputation d'être les meilleurs dans ce domaine et ils sont bien plus entreprenants que leurs "collègues" américains.

En règle générale, on peut introduire des virus dans n'importe quel ordinateur - des gros systèmes jusqu'à l'ordinateur familial. Pour cela, il suffit d'approcher et de se familiariser avec le système d'exploitation visé. La performance d'un virus dépend uniquement de l'habileté de son programmeur. Un virus, quel qu'il soit, n'est ni plus ni moins pervers que son concepteur. Selon les experts dans le domaine de la micro-informatique, il existerait à l'heure actuelle environ 50 à 100 virus différents. Les possibilités d'exploiter des virus dans un but constructif sont pratiquement inexistantes.

Même un prétendu "bon" virus destiné par exemple à comprimer un programme pour économiser la mémoire peut causer des ennuis s'il prolifère de façon incontrôlée. Et même les anti-virus, qui se propagent dans le seul but de rechercher et supprimer les virus destructeurs, peuvent échapper au contrôle.

Pour cette raison, nous devons utiliser les virus "positifs" avec une extrême prudence. Par exemple, le point de vue du lieutenant-colonel Erhard Haak développé début 1989 dans la presse militaire ouest-allemande, préconisait l'emploi des virus comme un moyen de combat préventif, une mesure de dissuasion en quelque sorte. Mais bien heureusement, les utilisateurs, même profanes, ne se trouvent plus tout à fait démunis face aux dangers des virus informatiques.

Grâce aux programmes de détection et de destruction de virus, comme par exemple le programme VIRtuel pour Atari ST fourni avec cet ouvrage, on peut désormais repérer les virus à temps, avant qu'ils n'aient provoqué des dégâts trop importants. Pour faire face à l'invasion croissante des virus, l'université de Hambourg a créé un centre d'épidémie virale qui a pour objectif de recenser et d'étudier toutes les espèces de virus existantes, de constituer une documentation complète et de mettre en oeuvre des moyens de

protection appropriés. Dans le cadre de ce projet, le centre de Hambourg a lancé un appel à tous les utilisateurs de micro-ordinateurs pour qu'ils leur fassent parvenir les virus dont ils ont été victimes.

❐ 1.1. Les dangers

L'un des principaux dangers qui émanent des virus réside dans la possibilité d'introduire dans un ordinateur des séquences de programmes manipulants qui opèrent des modifications tout à fait imperceptibles. Un tel virus pourrait, dans un service du personnel par exemple, modifier certaines données sur les employés au profit ou au détriment d'autres personnes. En tant que programme, le virus peut en réalité opérer n'importe quelle manipulation.

Le virus peut modifier, fausser ou remplacer librement tous les processus ou exécuter des tâches tout à fait différentes. Imaginons un virus capable de codifier un ensemble de données de telle sorte, qu'elles ne pourront plus être déchiffrées sans son concours. A chaque opération de lecture effectuée par le programme, les données seraient alors reconverties par le virus sous une forme exploitable, de telle sorte que l'utilisateur ne s'en apercevrait même pas.

Imaginons maintenant que le virus disparaisse au bout d'un an, laissant les programmes utilisateurs dans l'incapacité de traiter les données manipulées. Dans ce cas, même les copies de sauvegarde ne seront plus d'aucun secours, car toutes les sauvegardes réalisées durant cette année auront subi le même traitement. Il n'y a donc plus rien à faire.

Un tel incident nous conduirait tout naturellement à une remise en question radicale de l'utilité d'un système informatique. Les micro-ordinateurs les plus répandus s'exposent à toutes formes de sabotage extrêmement efficaces, car leurs systèmes d'exploitation ne comportent aucun dispositif de sécurité. Le danger que représentent les systèmes d'exploitation non-protégés pour l'activité humaine et même pour la santé des utilisateurs est à peine concevable.

Mais les données et les programmes ne forment pas l'unique cible des virus informatiques - le matériel peut également être endommagé ou même détruit. Les dégâts potentiels sont inestimables. Les experts dans ce domaine ont identifié deux catégories de virus particulièrement destructeurs :

- Les virus qui, jour pour jour, opèrent des modifications tout à fait insignifiantes dans la mémoire de l'ordinateur

- Les virus qui détruisent les données selon un principe aléatoire. Le système perd sa fiabilité et il ne restera plus qu'à l'arrêter sans que l'on puisse identifier l'origine de l'erreur.

Le fait de savoir si les données confidentielles enregistrées dans l'ordinateur d'une compagnie d'assurances ou d'une banque ou même dans le système de pilotage d'une centrale nucléaire sont aussi vulnérables face à une épidémie virale, nous conduit inévitablement à une remise en question fondamentale de l'utilité des ordinateurs dans ces domaines.

En principe, il est possible d'introduire des virus dans n'importe quel ordinateur. Dans cette optique, le principal facteur d'insécurité reste malgré tout l'homme, car c'est lui qui en dernier lieu, prend l'initiative d'introduire un virus à tel ou tel endroit. Les experts en matière de sécurité informatique s'accordent à dire que le plus grand danger vient de l'intérieur, du côté des initiés. Pour cette raison, les spécialistes doutent qu'il soit un jour possible de développer un moyen de protection d'une efficacité absolue pour lutter contre les virus.

Un ordinateur devient vulnérable dès qu'il est intégré à un réseau ou offre la possibilité de manipuler des séquences de programmes de l'extérieur, ce qui fait d'ailleurs tout son intérêt. C'est également l'avis de Rüdiger Dierstein du Centre Allemand de Recherche Aérospatiale, qui estime que le plus grand danger réside dans les actes de sabotage potentiels commis de l'intérieur et notamment par les collaborateurs qui disposent de droits d'accès légaux au système informatique.

Nous ne devrions pas arriver au point de couper le contact avec les autres ordinateurs par crainte d'une éventuelle contamination ; au contraire, nous devrions communiquer avec les autres et contrôler

soigneusement tous les chemins empruntés par les données pour pénétrer au coeur du système, de façon à empêcher tout au moins une éventuelle contamination. Les systèmes constitués en réseau offrent les meilleures conditions pour la propagation de virus.

Etant donné la possibilité d'accéder et d'introduire des données rapidement et de façon plus ou moins anonyme dans les programmes situés à distance, le virus trouve dans les réseaux un terrain extrêmement fertile et sa propagation peut prendre l'allure d'une explosion.

L'existence de nos jours d'ordinateurs accessibles au public - universités, écoles, bibliothèques, etc... - offre à un programmeur de virus la meilleure solution pour rester anonyme, d'autant plus que ces ordinateurs publics sont en règle générale connectés à d'autres calculateurs. Il est pratiquement impossible d'identifier le terminal qui a servi à introduire un virus dans le réseau.

Après une étude approfondie des conditions d'exploitation réalisée dans les centres de calcul des instances préfectorales ouest-allemandes, Dr. Klaus Brunnstein, professeur en informatique appliquée à Hambourg conclut que les gros systèmes des services publics sont tout aussi vulnérables face au danger potentiel des programmes manipulants.

Après avoir découvert de nombreuses failles dans les dispositifs de sécurité en place, il arriva à la conclusion que les services publics n'attachent pas suffisamment d'importance à la sécurité des données. Le professeur Brunnstein estime, tout comme ses collègues, qu'à l'heure actuelle, le plus grand danger se trouve dans les réseaux.

Contrairement aux grandes entreprises et institutions qui disposent, bien heureusement, de services compétents chargés d'assurer la sécurité des données et de protéger les systèmes contre l'intrusion de "petits malins" et de programmes viraux, les systèmes et les micro-ordinateurs utilisés dans certaines entreprises de taille moyenne semblent relativement peu protégés. Dans la plupart des cas, les systèmes d'exploitation des micro-ordinateurs constitués partiellement en réseau, n'offrent pas la possibilité de définir des droits d'accès en lecture et en écriture réservés à un nombre limité de personnes disposant d'une autorisation spéciale.

Ils partent du principe que tout utilisateur, une fois admis sur un système, doit être autorisé à effectuer toutes les opérations possibles. La meilleure solution serait de définir un droit d'accès pour chaque type de transaction opéré. Cela signifie toutefois qu'il faudrait abandonner les dispositifs de contrôle centralisés, tels qu'ils existent actuellement sur la plupart des micro-ordinateurs, au profit d'un système de contrôle décentralisé, réunissant plusieurs dispositifs de sécurité ; mais pour cela, il faudrait mettre au point une nouvelle génération de systèmes d'exploitation.

Cependant, le danger d'une épidémie virale ne réside pas uniquement dans la difficulté de maîtriser l'ensemble d'un réseau. Avec un peu d'adresse, on peut dissimuler totalement l'origine du virus. A cela s'ajoute la possibilité de faire disparaître le programme porteur après un premier lancement, sans toutefois briser la chaîne de l'infection. Par conséquent, toute conclusion pouvant mener au coupable serait rendue extrêmement difficile sinon impossible.

Bien sûr, il existe encore des ordinateurs qui travaillent de façon autonome, sans être directement connectés à d'autres systèmes. Cette catégorie réunit la plupart des ordinateurs personnels et familiaux qui seraient à l'abri des virus s'ils n'étaient pas entièrement tributaires d'un échange permanent de données et programmes à l'aide de disquettes.

Même en utilisant des programmes originaux distribués par les sociétés de logiciels, le risque de contamination n'est pas totalement exclu, puisque ces sociétés se trouvent en contact permanent avec d'autres utilisateurs qu'elles chargent de tester les logiciels.

Cependant, l'échange privé de disquettes et l'utilisation de programmes qui relèvent du domaine public constituent une source d'infection privilégiée étant donné qu'ils garantissent un degré d'anonymat relativement élevé, qui fait baisser le seuil de dissuasion en ce qui concerne les délits informatiques. Il en est de même pour les boîtes aux lettres, très répandues dans les cercles privés d'utilisateurs. Qui connaît vraiment tous ceux qui peuvent y accéder ? Les programmes infectés en provenance des boîtes aux lettres ont déjà fait de nombreuses victimes parmi les utilisateurs qui ont dû parfois assister à la paralysie totale de leurs ordinateurs.

❒ 1.2. Conséquences

Les conséquences entraînées par un programme de virus sont si complexes, qu'il est pratiquement impossible d'en exposer toutes les facettes. Nous allons donc nous limiter à un certain nombre de cas d'infection qui ont réellement eu lieu ou que nous avons imaginés selon un scénario possible aussi bien dans le présent que dans l'avenir.

Cependant, on ne peut pas affirmer avec certitude toutes les anomalies que nous avons citées sont le résultat d'une manipulation virale. Certains incidents peuvent être dûs à une fausse manipulation, un programme défaillant ou un matériel défectueux. Il y a davantage de claviers détruits par une tasse de café renversée que par des virus.

Il est bien évident que les effets mentionnés ci-dessous ne se manifestent pas simultanément. Certains virus ou programmes proches de virus ne font qu'exécuter une tâche bien définie. Mais il est tout à fait essentiel d'observer son ordinateur, car la moindre modification dans son comportement peut fournir des indices précieux sur la présence éventuelle d'un virus. La liste suivante réunit les principaux symptômes qui se manifestent à la suite d'une manipulation d'origine virale :

- Les programmes s'exécutent plus lentement que d'habitude
- Les programmes effectuent des accès au disque dur et aux disquettes qu'ils n'opéraient pas auparavant.
- Les délais de chargement des programmes ou fichiers s'allongent
- Le système se bloque sans raison apparente
- Certains programmes qui se laissaient charger jusqu'ici sans aucune difficulté sont interrompus avec le message d'erreur "Mémoire insuffisante"
- Des messages d'erreur inconnus ou inexplicables s'affichent sur l'écran
- Sur la disquette ou le disque dur la place disponible diminue, alors qu'on ne rajoute ni modifie aucun fichier
- Les programmes résidents fonctionnent mal ou ne tournent plus du tout

- L'écran se vide totalement
- L'ordinateur est sans cesse réinitialisé
- Le clavier ne répond plus
- Les disques durs ou les disquettes sont reformatés
- Les index sont effacés
- Les pointeurs des programmes sont "déformés"
- Certaines routines système se dégradent
- Une quantité considérable de fausses données est générée pour surcharger le système
- L'ordinateur émet un ricanement sournois
- L'écran est effacé
- Le système effectue des virements bancaires à d'autres personnes
- Les comptes sont modifiés
- L'accès aux programmes est rendu difficile ou même impossible par la mise en place arbitraire d'une série de mots de passe
- Les données sont en grande partie modifiées et par conséquent, inutilisables
- Crash des têtes de lecture sur les disques durs
- Retours en arrière répétés du papier provoquant un bourrage dans l'imprimante
- Le virus MS-DOS inscrit sur les PC équipés d'une carte Hercules provoque un message ineffaçable sur la couche de phosphore du moniteur
- Le lecteur de disquettes fait retentir une mélodie, en provoquant des mouvements inconsidérés de la tête de lecture

❒ 1.3. Historique

Retracer l'histoire des virus informatiques dans son ensemble n'est pas chose facile, car la plupart des virus ont été spécialement conçus pour éviter autant que possible de se faire repérer ou de dévoiler leurs mécanismes de propagation. Ceci nous amène à penser que les virus informatiques existaient bien avant que l'on ne commence à en prendre conscience et à en parler dans la presse.

D'autre part, il convient de noter que la découverte de nouveaux virus dépend essentiellement de la qualité de programmation. Les

virus détectés récemment n'ont pu être identifiés qu'en raison de leur médiocrité. Les virus bien programmés n'ont vraisemblablement jamais pu être repérés. La fréquence d'apparition de certains virus ne constitue pas un critère fiable permettant d'établir avec certitude la présence et l'ampleur réelle des virus mis en circulation. Pour être plus directs, on pourrait même prétendre que les programmes de virus sont de plus en plus médiocres.

Les seuls indices dont nous disposons à l'heure actuelle nous ont été fournis par les documents qui rendent compte des épidémies virales dans le monde informatique. Malheureusement, ces documents sont le plus souvent publiés une fois que les virus ont provoqué des dégâts irréparables. Les premiers virus ont vraisemblablement été mis au point par des programmeurs de gros systèmes - cela semble logique, si l'on pense que les gros systèmes existaient bien avant les ordinateurs personnels. Les programmeurs travaillant sur les gros systèmes avaient déjà quelques longueurs d'avance en ce qui concerne la technique de programmation, alors que dans le domaine de la micro-informatique il restait encore un long chemin à parcourir. Il est difficile après coup d'affirmer avec certitude si les virus ont été développés à l'origine par plaisanterie, sous couvert d'une mission de recherche, comme un acte de vengeance personnel ou pour d'autres raisons encore.

L'avènement des ordinateurs personnels qui sont peu à peu devenus accessibles aux particuliers a permis aux programmeurs des gros systèmes d'appliquer et de développer leurs connaissances sur ces "petits" ordinateurs pour les transmettre ensuite à d'autres programmeurs.

Mais le problème des virus n'a été connu du public qu'à la suite des expériences menées par Fred Cohen, qui ont montré de façon spectaculaire les conséquences d'un tel programme de virus. Le "Program Virus" développé par Cohen fin 1983, parvint au bout de cinq tentatives à infecter en une heure seulement tous les programmes qui se trouvaient dans l'ordinateur VAX 11/750 de l'université de la Californie du Sud.

Lors d'une expérience ultérieure, qui, on le comprend, n'a pu être réalisée à l'université de la Californie du Sud, où Cohen se vit retirer toute autorisation d'accès au système informatique, le délai

d'infection des programmes stockés dans l'ordinateur n'était plus que de 20 secondes. Le virus était imperceptible, étant donné qu'il se résumait en quelques lignes de code machine.

Le code viral fut introduit dans l'ordinateur au moyen d'un programme porteur et parvint au système central de pilotage en simulant son appartenance à l'ordinateur. De là, il réussit à pénétrer dans la bibliothèque de logiciels et finit par infecter tous les autres programmes qui lui avaient jusque-là échappé.

Le virus développé par Cohen était un "virus hibernant", capable de somnoler pendant un long moment à l'intérieur de l'ordinateur en attendant un événement précis pour se déclencher, comme par exemple un mot de code ou une date pré-définie. Lorsque l'événement attendu se produit, le virus passe à l'action en exécutant une commande cachée.

Les expériences réalisées par Cohen sur les gros ordinateurs ont montré que les programmes de virus pouvaient se propager à une allure vertigineuse par des voies tout à fait légales et que tous les utilisateurs dotés de privilèges élevés étaient des porteurs de virus en puissance.

Cohen considérait les systèmes multi-utilisateurs comme étant particulièrement menacés car les données étaient partagées de la même façon que dans un réseau. A la suite de ces expériences, les rapports sur les cas d'épidémie virale se sont multipliés dépassant cette fois-ci le cadre des périodiques spécialisés.

Le 13 mai 1988, à la veille du 40ème anniversaire de l'état d'Israël, un virus que l'on a baptisé "le virus israélien" détruisit toutes les données des micro-ordinateurs sous MS-DOS auxquels il put accéder, provoquant ainsi des dégâts très importants.

Les premiers symptômes de ce virus se sont fait sentir, début 1988, dans l'ordinateur central de l'université hébraïque de Jérusalem lorsqu'on s'aperçut que certaines tâches qui s'exécutaient habituellement en 3 minutes, prenaient soudain plus de 15 minutes et que l'activité de l'ordinateur se ralentissait de jour en jour. Au bout de 30 minutes environ, le virus avait ralenti le système d'environ un cinquième de sa vitesse normale en affichant de temps à autre des faux résultats.

Etant donné que le programme de virus présentait certaines erreurs de forme, il a pû être détecté à temps ; en effet, certains fichiers (.COM) ont été infectés une seule fois, d'autres fichiers par contre (EXE) ont été contaminés à plusieurs reprises ; à chaque infection, la taille des fichiers augmentait de 1800 octets. Un groupe de travail composé de programmeurs, étudiants et professeurs parvint à développer un antivirus qui fut distribué à toutes les personnes concernées, accompagné d'une mise en garde.

Mais avant d'être repéré, le virus avait déjà détruit l'un après l'autre tous les résultats de recherches auxquels il avait pu accéder à partir du système central. Six mille gros ordinateurs disséminés dans le monde entier étaient sérieusement menacés, car le virus ne se limitait pas au seul territoire d'Israël. Il gagna les Etats-Unis par le biais d'un réseau international, d'où il menaçait de contaminer environ 200 centres de recherche ouest-allemands à travers le système d'échange de données "EARN" qui couvre le monde entier. Même les ordinateurs de la défense nationale et des services de sécurité ne lui auraient échappé.

Aux Etats-Unis, un autre virus, que l'on a baptisé RTM, devait provoquer, au mois de novembre 1988, des dégâts d'environ 96 millions de dollars. Grâce aux réseaux "Arpanet" et "Milnet", il parvint à contaminer en quelques heures seulement plusieurs milliers d'ordinateurs appartenant à des universités et instituts de recherche.

Un certain nombre de virus RTM ont été découverts dans les ordinateurs du ministère de la défense, au laboratoire de l'IDS de Livermore en Californie, au centre de recherches nucléaires Los Alamos au Nouveau Mexique, aux Laboratoires Lincoln de la base aérienne Hanscom dans le Massachusset et au centre de recherche de la NASA près de San-Francisco. Les risques de propagation du virus ont motivé les services du FBI à ouvrir une enquête sans plus attendre.

Devant cette menace, les autorités ont organisé une réunion secrète à laquelle ont participé non seulement des fonctionnaires de la NASA et du FBI, mais aussi des représentants du ministère à l'énergie atomique, quelques officiers de l'armée de l'air et membres du laboratoire de recherches en balistique, ainsi que des professeurs d'université. Comme il a été révélé par la suite, on décida lors de cette conférence de créer une centrale pour

rassembler tous les virus repérés et prendre les mesures de protection appropriées.

Fort heureusement, le virus qui avait provoqué cet incident était un "virus positif", développé et propagé par Robert Tappan Morris (RTM), un jeune homme de 23 ans. Robert Morris avait lancé son virus à partir de l'université de Cornell le jour où un super ordinateur de type IBM 3090-600 E allait être connecté au réseau en présence d'environ 250 scientifiques, représentants de l'industrie et politiciens.

Le père de Robert Morris fut l'un des meilleurs experts en sécurité informatique dans cette branche. Il avait participé, en qualité de co-développeur du système d'exploitation UNIX, à la mise au point d'un procédé de chiffrage de mots de passe. Déjà au début des années 60, il avait développé, en collaboration avec quelques autres chercheurs des Laboratoires Bell, un jeu appelé "Darwin" qui avait pour tâche d'attaquer et d'engloutir tous les programmes des joueurs.

Le "virus de Darwin" ne fut rendu public qu'au début des années 80, lorsque M. Morris senior révéla le secret à la commission d'enquête constituée à la demande du congrès des Etats Unis. A cette occasion, il déclara que les systèmes de sécurité des plus grandes entreprises américaines et de l'armée étaient inviolables, car ils avaient été conçus par les meilleurs spécialistes.

C'est à l'âge de 11 ans que Robert Morris junior eut son premier contact avec les ordinateurs. En 1983 il s'inscrit à l'université de Harvard. En 1985, il entrait pour un an dans une société informatique texane spécialisée dans la programmation de systèmes de sécurité, après quoi, il se vit attribuer le poste de responsable d'exploitation adjoint dans le centre informatique Aiken de Harvard et reçut tous les privilèges de super-utilisateur liés à cette fonction, qui lui donnaient tous les droits d'accès au système informatique.

La carrière de Morris confirme une fois de plus le point de vue défendu par la plupart des spécialistes, qui affirmaient que le principal danger vient le plus souvent de l'intérieur, de ceux qui possèdent tous les droits d'accès possibles à un système

informatique, et que certains spécialistes se faisaient duper par leurs propres collègues.

Morris transmit son programme de virus par l'intermédiaire d'une messagerie appelée "SendMail" utilisée pour communiquer avec le laboratoire de recherches informatiques de Boston, à travers le réseau Arpanet, géré par le Pentagone. Finalement, c'est par une porte dérobée, laissée ouverte par les concepteurs du programme "SendMail" pour pouvoir y accéder à tout moment, que le virus franchit les barrières de sécurité. Il ne lui restait donc plus qu'à se procurer un statut de programme lui permettant d'être traité par l'ordinateur.

Les ordinateurs de Sun et Vax ont perçu le programme de virus comme un logiciel personnalisé et l'ont laissé lire toutes leurs listes de clients. Pour parvenir aux mots de passe des utilisateurs, Morris junior avait mis au point un dictionnaire standard chiffré, grâce au programme de déchiffragde éveloppé par son père sur UNIX.

Muni de cette liste, le programme se mit alors à comparer les mots chiffrés avec les noms des utilisateurs. Chaque fois qu'il trouvait le mot d'accès juste, il se multipliait à l'intérieur du système respectif. Une erreur qui s'était glissée dans la fonction Arpanet favorisait davantage la propagation du virus.

Chaque fois que le virus pénétrait un nouveau système informatique, il vérifiait dans un premier temps si l'ordinateur n'était pas déjà contaminé pour éviter de l'infecter une seconde fois. En définitive, un ordinateur sur 10 fut infecté de cette manière, car le virus avait écarté toute possibilité de protection.

Une autre épidémie, qui témoigne de l'extraordinaire vitesse de propagation des programmes viraux, a été déclenchée par le "virus de Noël". Un étudiant de l'université scientifique de Clausthal en Allemagne Fédérale, voulait sans doute faire une plaisanterie à ses amis du système central d'IBM. Il eut alors l'idée de leur envoyer un programme qui les invitait à entrer la chaîne de caractères CHRISTMAS avec le message "laissez tourner ce programme et amusez-vous bien" !

Une fois cette instruction exécutée, l'écran affichait un joli sapin de Noël, tandis qu'à l'arrière-plan, le programme continuait à transmettre le même message à toutes les adresses répertoriées

dans les annuaires électroniques des utilisateurs. Malheureusement, le plaisantin n'avait pas réalisé que l'université était reliée à EARN-BITNET, un réseau scientifique international.

A cette époque, ce réseau composé de gros ordinateurs comptait environ 500 noeuds en Europe, 1500 aux Etats Unis et environ 2000 noeuds disséminés à travers le monde. Cependant, le programme ne toucha qu'environ 50% des noeuds, étant donné que les autres systèmes d'exploitation présents sur le réseau n'étaient pas en mesure de traiter le message. Parti d'Allemagne Fédérale le 9 décembre 1987 à 12H45, le "sapin de Noël" fit le tour du monde en très peu de temps. Pour illustrer son extraordinaire vitesse de propagation, voici les premières stations de son périple :

Heure	Noeud
12H43	Université de Houston
12H44	Université d'Utah
12H44	Université catholique de Nijmegen
12H44	Université de la Californie du Sud
12H44	Université Nationale de Singapore
12H45	City University de New-York
12H45	Institut de technologie de Monterrey
12H46	Université technique de Twente
12H46	Université technique de Danemark
12H46	Institut Weizmann en Israël
12H47	Centre informatique de l'université de la Louisiane

Un autre cas d'infection connu du public a été déclenché par un virus qui était destiné à l'origine à une entreprise située à Dallas mais qui finit par détruire les bases de données de plusieurs organes gouvernementaux. Le virus a attaqué entre autres environ 100 ordinateurs de la NASA à Washington, Maryland et en Floride. La destruction des données par le virus a entraîné des retards considérables dans la plupart des projets mis en place par les autorités.

Le premier forum qui s'est tenu sur le thème des virus informatiques touchant aux micro-ordinateurs fut organisé par le CCC de Hambourg (Chaos Computer Club), fin décembre 1988. Selon les organisateurs, ni les fabricants de systèmes d'exploitation et de logiciels ni les sociétés de développement, ni même les

concepteurs de logiciels n'avaient su - ou n'ont pas voulu - reconnaître le problème soulevé par l'invasion des virus et cela malgré les nombreuses publications parues sur ce sujet. Pour cette raison, le congrès annuel du Chaos fut entièrement consacré aux virus informatiques.

Le débat qui s'est ouvert à cette occasion avait été motivé en outre par l'arrivée massive en RFA, vers le milieu de l'année 1986, d'une série de programmes en provenance des Etats-Unis qui étaient infectés par le virus PC. Le débat avait également pour objectif de sensibiliser l'opinion face à cette situation et de rassembler et diffuser des témoignages sur ses conséquences, ses effets et les possibilités de protection.

Parmi les 200 à 300 participants au congrès se trouvaient, selon les organisateurs, une vingtaine de programmeurs possédant une expérience pratique des virus. Au centre du congrès on a pu assister à la présentation d'un virus pour MS-DOS, VIRDEM.COM, développé par Ralf Burger. VIRDEM.COM était un virus relativement inoffensif qui ne visait pas à détruire les programmes mais se contentait d'ajouter une fonction supplémentaire et n'utilisait qu'un lecteur de disquettes pré-défini pour se multiplier.

A travers cette expérience, Ralf Burger voulait démontrer à quel point un utilisateur était impuissant face à une infection virale, mais en même temps, elle offrait à n'importe quel programmeur sous MS-DOS, même inexpérimenté, la possibilité de mettre en circulation une version modifiée de ce virus.

Dans son numéro d'avril 1987, un périodique spécialisé ouest-allemand mettait en garde contre une version modifiée du programme VIRDEM.COM qui se trouvait en circulation. Son auteur avait redéfini la spécification du lecteur, en remplaçant l'unité A: par l'unité C:. Ainsi modifié, le virus de démonstration était en mesure de porter de graves préjudices aux utilisateurs.

Depuis cet incident, la presse informatique ne cesse de publier des articles sur le thème des virus. Certains sont même allés jusqu'à publier des programmes de virus intégralement, sous forme de listings. Ralf Burger, qui fut l'artisan du virus de démonstration VIRDEM.COM, a publié, en 1987, un ouvrage consacré aux virus.

Parallèlement, on a développé toute une série de programmes de protection contre les virus disponibles gratuitement dans le domaine public. D'autre part, le Salon Atari 1988 a permis de prolonger le débat sur ce sujet. Ainsi, lors d'un forum dirigé par Dr. Klaus Brunnstein, professeur en informatique appliquée à l'université de Hambourg, un débat publique eut lieu sur le thème des virus informatiques avec la participation d'un certain nombre de représentants des plus grands fabricants de logiciels.

Après une brève introduction à la problématique des virus, on a reproché aux périodiques spécialisés d'avoir donné trop de détails sur les virus, en publiant par exemple des programmes viraux sous forme de listings. Les publications sur les différentes épidémies virales ayant fait de nombreuses victimes parmi les grands fabricants de logiciels, cela aurait contribué d'une part à insécuriser les utilisateurs et d'autre part, à stimuler les programmeurs de virus, en leur montrant les préjudices engendrés par tel ou tel virus.

Nous voulons toutefois rassurer le public, car depuis ce temps les fabricants. de logiciels ont bel et bien reconnu le problème et commencent à présent à développer des protections internes contre les virus. Le dommage rend plus sage. A l'heure actuelle, aucun programme n'est en mesure d'assurer une protection absolue ; par exemple, les programmes de protection sur Atari couvrent uniquement les virus qui attaquent les boot-secteurs.

C'est tout à fait par hasard qu'une société informatique découvrit, en mai 1988, un virus sur la disquette contenant un logiciel pour Atari ST. Ce virus n'était pas sans danger car il avait pour tâche d'écrire son propre code par-dessus la protection en écriture de certains programmes, qui se trouvait dans le boot-secteur.

Lorsque le virus fut détecté, 1500 sur les 10000 exemplaires imprimés avaient déjà été distribués et ont dû être repris. Etant donné que la disquette était fermement attachée au livre, il a fallu oter et recoller l'emballage pour supprimer le virus qu'elle contenait.

Cependant, les ordinateurs Atari ne sont pas les seules victimes. Un virus implanté par plaisanterie lors d'une expérience inoffensive sur Apple-Macintosh a fait de sérieux ravages aux Etats-Unis, au Canada et même en Europe. Les auteurs, une équipe de

programmeurs pour un magazine informatique canadien, ont voulu mesurer l'ampleur du piratage dans le domaine des logiciels.

Le programme, qui s'est propagé grâce à un téléservice, avait pour tâche de lire l'horloge système et afficher un message à la date du 2 mars avant de s'auto-détruire. Le jour de l'anniversaire de Macintosh II, tous ses utilisateurs devaient recevoir un message de paix sur leur moniteur.

Mais ce virus n'était nullement inoffensif car il finissait par détruire l'ensemble du système d'exploitation et les fichiers de données.

❒ 1.4. Définition des virus

En ce qui concerne les virus informatiques, il n'existe à l'heure actuelle aucune définition universellement reconnue. Nous allons nous appuyer sur l'essai de définition entrepris par R. Burger dans son livre, car à l'heure actuelle, il constitue l'ouvrage de référence le plus répandu sur ce sujet :

> "Un programme doit être considéré comme un virus s'il réunit les propriétés suivantes :
>
> **1**. Il modifie des logiciels extérieurs par inclusion de ses propres structures dans les logiciels
>
> **2**. Les modifications qu'il provoque ne se limitent pas à un seul logiciel mais touchent au moins un groupe de programmes
>
> **3**. Il sait reconnaître si un logiciel a déjà été infecté
>
> **4**. S'il reconnaît un logiciel déjà modifié, il s'interdit de procéder à une nouvelle modification
>
> **5**. Le logiciel infecté présente désormais les quatre propriétés mentionnées ci-dessus
>
> Si un programme ne possède pas simultanément toutes ces propriétés, il ne peut pas être considéré comme un virus au sens le plus strict du terme".

En d'autres termes, pour être qualifié de virus, un programme doit être capable de se multiplier à travers les modifications qu'il opère sur les autres programmes (cf. points 1, 2 et 5). De plus, un virus

doit savoir reconnaître ces modifications (cf. point 3) pour ne pas renouveler la manipulation sur des programmes déjà modifiés (cf. point 4). Cependant, cette définition nous livre entre les lignes quelques informations supplémentaires et révèle en même temps un certain nombre de points obscurs :

❶ Selon cette définition, un programme de virus ne porte pas forcément en lui une tâche de manipulation. Le simple fait de se propager peut constituer, pour ainsi dire, un but en soi. D'accord ! Après tout, pourquoi pas ?

❷ Tel qu'il a été défini, le virus se contente d'inclure ses propres structures dans les logiciels. Mais pourquoi devrait-il se limiter à ses propres structures ?

Il serait tout à fait possible de combiner plusieurs éléments provenant de logiciels tout à fait différents pour les inclure dans la structure du programme manipulé.

❸ Cette définition ne tient pas compte des possibilités d'évolution sur plusieurs générations.

Qu'est-ce qui pourrait bien empêcher un virus de modifier un programme à plusieurs reprises ? Imaginons par exemple un virus qui possède la faculté de se modifier de génération en génération en assimilant, par exemple, certaines données à partir des ordinateurs déjà infectés. De cette façon, il pourrait manipuler un programme déjà infecté en y incluant la nouvelle version de son code.

Un tel virus pourrait porter en lui un certain nombre d'informations spécifiques précisant qu'il n'a pas été en mesure de remplir sa mission et générer, sur la base de ces informations, d'autres virus qui chercheraient à accomplir sa mission d'une façon différente. Si l'un de ses "descendants" ne parvenait pas à exécuter sa tâche, le virus "parent" aurait la possibilité de corriger les "informations génétiques" qu'il lui a transmises.

De cette façon, un seul et même virus pourrait engendrer plusieurs variantes correspondant aux différents stades de son évolution sur un système donné. Sur un système de conception différente, le même virus pourrait générer d'autres variantes encore, en fonction

des conditions spécifiques offertes par le système en question. Ce type de programme appartient à la catégorie des virus évolutifs que nous allons examiner de plus près dans le chapitre suivant. Les virus évolutifs, n'héritent pas une tâche de manipulation précise, mais plutôt un mécanisme de propagation spécifique. Pourrait-on, dans ce cas précis, parler de virus intelligents ?

Selon la définition de Burger, ce type de programme n'entrerait pas dans la catégorie des virus car, bien qu'il ait identifié une infection précédente, il procède à une nouvelle modification. On pourrait prétendre toutefois que le processus d'évolution génère plusieurs programmes et qu'à ce titre, la définition en tient compte.

Mais alors, il faudrait déterminer à partir de quel moment on peut considérer deux programmes comme étant identiques. Avant de faire une comparaison, nous devons en définir les critères : faut-il que tous les octets soient identiques et rangés de la même façon pour que l'on puisse parler de virus identiques ou bien, ne faudrait-il pas plutôt remettre en question la démarche théorique qui perçoit le virus comme une structure isolée ? Dans cette optique, il faudrait intégrer à la notion de virus tous les stades possibles d'une éventuelle mutation pour que l'on puisse enfin considérer le principe de base d'un virus, autrement dit, le fondement de sa structure spécifique comme un critère de similitude.

Ceci nous amène à soulever une question d'ordre philosophique sur le sens d'une éventuelle "vie de l'ordinateur" qui nous conduirait inévitablement à faire une parallèle entre les virus informatiques et les virus biologiques et peut-être même à découvrir des similitudes dans leurs mécanismes de reproduction. Ce serait sans aucun doute un sujet très intéressant mais il dépasse largement le cadre de ce livre.

La nécessité de définir des critères de similitude dépend en dernier lieu de l'objet auquel pourrait s'appliquer une telle définition. Laissons donc au programmeur le soin de décider de quelle façon il veut faire reconnaître à son virus un programme déjà infecté, car c'est bien sa finalité. Il n'en reste pas moins que la définition des virus manque de précision sur ce point.

D'autre part, la définition de R. Burger néglige un fait essentiel : l'identification pure et simple d'une manipulation accomplie ne constitue pas à elle seule un indice fiable sur la nature du virus ;

il faudrait également reconnaître la génération du virus qui est à l'origine de cette manipulation pour savoir s'il a évolué.

La plupart des programmes de virus ne font pas cette distinction de façon explicite car ils n'évoluent pas et de ce fait, il ne présentent qu'un seul et unique stade d'évolution ; cela signifie que le virus qui est à l'origine de la manipulation détectée ne sera pas modifié.

Cette réflexion est intimement liée au fait de savoir si les générations d'un virus doivent être considérées comme étant des virus identiques ou différents. Cette distinction explicite n'entre en ligne de compte qu'à partir du moment où les ascendants et descendants possèdent eux-mêmes la faculté d'évoluer. Je propose donc de compléter la définition de Burger comme suit :

Un programme doit être considéré comme un virus s'il réunit les propriétés suivantes :

❶ Il modifie des logiciels extérieurs par inclusion d'une structure différente dans ces logiciels

❷ Les modifications qu'il provoque ne se limitent pas à un seul logiciel mais touchent au moins un groupe de programmes

❸ Il sait reconnaître si un logiciel a déjà été infecté, et identifie le stade de l'évolution du virus qui l'a infecté

❹ S'il reconnaît un logiciel déjà modifié, il décide de procéder ou non à une nouvelle modification

❺ Le logiciel infecté présente désormais les propriétés cités aux points 1 à 4.

Chapitre 2

Les différentes catégories de virus

Dans ce chapitre, nous allons tenter d'établir une classification approximative des virus, qui ne prétend être ni exhaustive, ni universelle. Pour ne citer qu'un exemple, un groupe de travail de Santa-Clara engagé dans la lutte anti-virus est parvenu à isoler et identifier 39 familles de virus avant juin 1988. Mais depuis cette date, de nombreux autres virus ont été découverts. Steve Gibson, spécialiste américain en logiciels a divisé les virus informatiques en quatre familles :

- GPIV (General Purpose Infector Virus) : Cette catégorie regroupe les virus à caractère universel qui se glissent au début ou à la fin d'un programme d'application. On les reconnaît en règle générale par une modification de la taille originale du programme. Certaines variantes plus subtiles possèdent la faculté de se dissimuler, de façon à n'éveiller aucun soupçon lors d'une vérification de la taille du programme.

- SPIV (Special Purpose Infector Virus) : Cette catégorie englobe les virus qui se glissent à un endroit précis du logiciel d'application. Pour cette raison, ils sont plus difficiles à éliminer.

- VGPIV (Very Clever General Purpose Infector Virus) : On retrouve dans cette catégorie un certain nombre de virus universels particulièrement astucieux qui réunissent les caractéristiques des deux premières familles, GPIV et SPIV. Ces

virus peuvent infecter, sans se faire repérer, tous les programmes d'un système, avant d'entrer en action. Par conséquent, les virus de cette catégorie sont les plus difficiles à combattre.

CSIV (Central System Infector Virus) : Les virus de cette catégorie ont pour but de pénétrer par le chemin le plus court au coeur du système d'exploitation pour déclencher, à partir de là, toute une série d'actions destructrices sur l'ensemble du système. Les virus de cette catégorie sont introduits en règle générale par l'intermédiaire d'un "Cheval de Troie".

Etant donné qu'il existe vraisemblablement un certain nombre de formes intermédiaires, les barrières qui séparent ces catégories de virus ne sont pas très distinctes. Ainsi, il est tout à fait possible de développer des link-virus qui réunissent les propriétés de plusieurs types de virus : virus batch, virus évolutifs, virus résidents en mémoire, virus n'écrivant pas par-dessus les programmes. De même, à défaut d'une définition généralement admise, toute tentative de différenciation, d'identification et de classification peut paraître quelque peu arbitraire.

Il existe toute une série de virus spécialisés qui ne se manifestent que sur certains types d'ordinateurs, car ils agissent sur les fonctions caractéristiques du systèmes d'exploitation. Par exemple, les boot-virus et de batch attaquent uniquement les systèmes dits "ouverts" qui chargent les programmes à partir d'un support externe au moment de l'initialisation.

D'autres virus en revanche utilisent des caractéristiques matérielles spécifiques et se limitent par conséquent à un type d'ordinateur particulier. La plupart de ces virus ont toutefois un point commun : ils se multiplient à l'intérieur du système et véhiculent une tâche de manipulation particulière qu'ils ne mettent à l'exécution qu'après avoir infecté bon nombre des programmes. De cette façon, ils ne peuvent pas être repérés avant d'entrer en action.

Certains programmes, comme par exemple les "vers" et les "Chevaux de Troie" que nous allons analyser dans ce chapitre, ne se laissent pas facilement intégrer dans la définition que nous avons commentée plus haut, car leur principal objectif n'est pas de se

reproduire de façon autonome mais plutôt de mettre en oeuvre une tâche de manipulation spécifique.

❐ 2.1. Boot-virus

Les boot-virus utilisent une caractéristique spécifique, qui consiste à charger, au moment de l'initialisation, un certain nombre d'informations supplémentaires internes au système, à partir d'un support de données connecté. Pour cette raison, ces virus se sont largement répandus sur Atari ST, sur tous les ordinateurs qui fonctionnent sous MS-DOS, sans oublier les systèmes Amiga et Macintosh. Pour infecter un ordinateur, le virus d'initalisation procède de deux façons différentes : soit il s'introduit dans le boot-secteur, d'où son nom, soit il se place dans la partie chargeable du système d'exploitation.

Ce virus oblige le boot-secteur à s'exécuter de façon autonome et se glisse dans la structure d'interruption de l'ordinateur. A chaque accès en lecture ou en écriture sur des disquettes saines, il se multiplie en écrivant son propre code dans le boot-secteur. Il procède de la même façon pour manipuler le système d'exploitation, mais dans ce cas, son action porte sur la zone réservée au système d'exploitation à l'intérieur d'une disquette. Dans cette catégorie figurent en première ligne les virus "Arc-en-Ciel", SCA, nVir et Scores.

Selon la classification de Steve Gibsons, le boot-virus appartient à la catégorie des virus CSIV. Nous allons approfondir cette espèce de virus dans le chapitre suivant.

❐ 2.2. Link-virus

Les link-virus doivent leur nom à leur faculté de s'introduire dans les autres programmes ou d'établir un lien avec eux (former une chaîne). Ce type de virus se glisse dans les programmes stockés sur une disquette. A chaque lancement du programme infecté, Il se déclenche et se cherche un petit coin tranquille pour exercer son action néfaste.

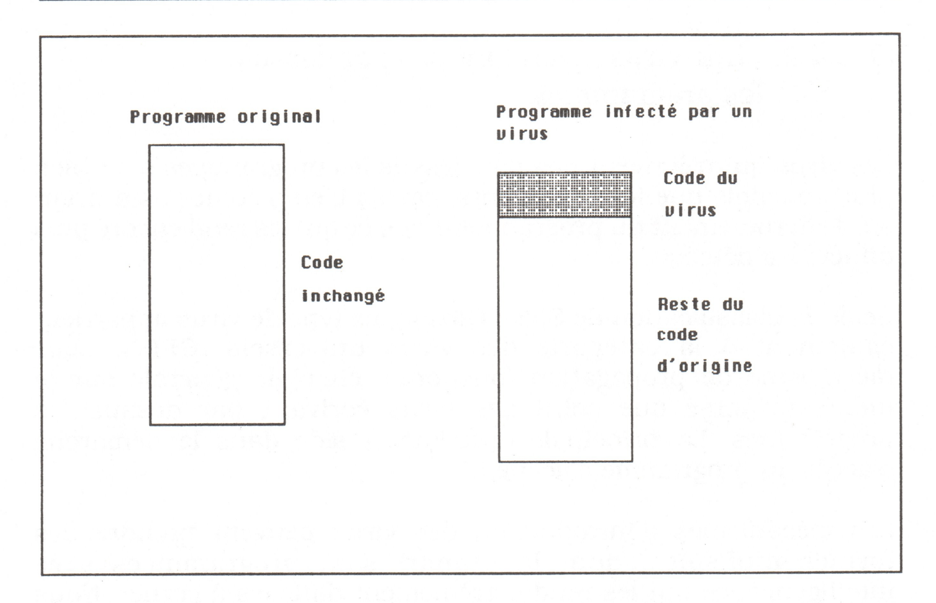
Les link-virus modifient en règle générale le ckecksum du programme d'origine mais cela dépend essentiellement de la méthode utilisée pour calculer le ckecksum : la façon la plus simple d'obtenir celui-ci est d'additionner tous les octets d'un programme (un programme est formé d'une suite de chiffres).

Les modifications opérées sur les octets ne se laissent pas trouver très facilement - si l'on ajoute une valeur à un octet en déduisant la même valeur d'un autre octet, le ckecksum et en dépit des modifications opérées sur le même code. Il existe toutefois un certain nombre d'algorithmes "intelligents", capables de repérer ce type de modification en effectuant le ckecksum.

❒ 2.2.1. Virus écrivant par dessus les programmes

Le virus écrivant par dessus les programmes constitue la forme la plus classique et la plus primitive des programmes viraux. Il détruit une partie du programme-hôte, sans qu'il soit possible de la reconstituer, en la remplaçant par son propre code. De ce fait, il ne peut pas être détecté de façon directe, car il ne modifie pas la taille, mais agit essentiellement sur le déroulement des programmes.

Malgré l'infection, certains programmes continuent à fonctionner normalement et ceci pour deux raisons : soit parce que le virus a été programmé avec astuce, soit parce que le programme infecté disposait dès le départ d'un espace mémoire inutilisé, qui offre un lieu d'accueil privilégié aux virus. Selon la classification de Steve Gibson, cette espèce de virus appartient à la catégorie GPIV.



Pour introduire un virus dans un système informatique, le premier programme est délibérément infecté et mis en circulation. Lorsqu'un programme infecté est lancé, la partie virale s'exécute en premier et se met à la recherche des programmes d'application en vérifiant l'index des supports de données accessibles (lecteurs de disquettes ou disques durs).

Lorsqu'il trouve un programme, il charge un fragment dans la mémoire de travail et vérifie s'il contient l'empreinte virale caractéristique pour savoir si celui-ci a déjà été infecté.

L'empreinte virale est constituée par une instruction de saut spécifique du virus, une opération neutre ou un chiffre "magique". Si le programme examiné est déjà infecté, le virus poursuit sa recherche jusqu'à ce qu'il trouve un programme qui ne comporte pas l'empreinte virale caractéristique.

Lorsque le virus trouve un programme sain, il s'y introduit en apposant sa copie au début de l'enregistrement du programme dans la mémoire de masse. Les programmes contaminés transmettent le virus suivant le même schéma ou exécutent à un moment donné une tâche de manipulation pré-définie, qui consiste, par exemple, à détruire les données. L'infection se poursuit ainsi jusqu'au dernier programme accessible à l'intérieur du système.

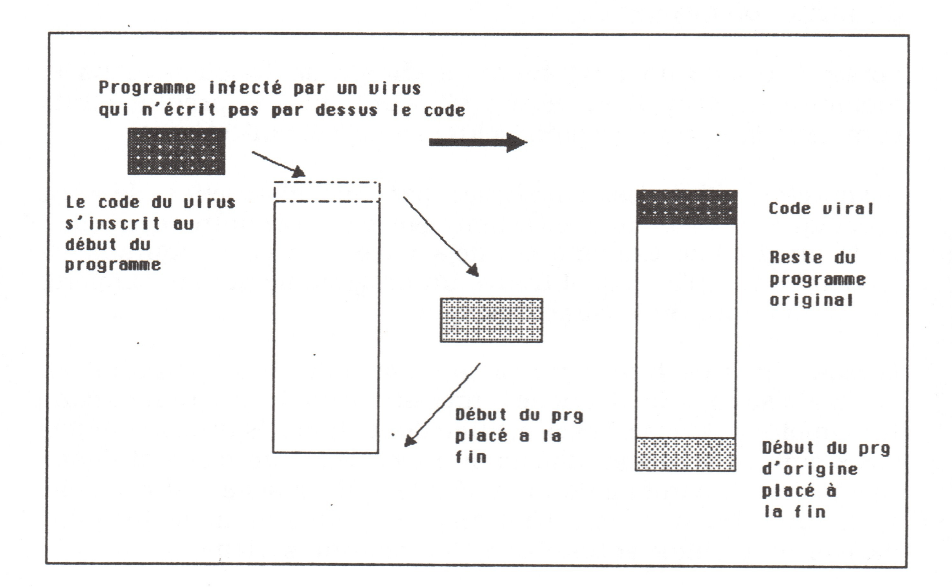
❒ 2.2.2. Link-virus n'écrivant pas par dessus les programmes

Les virus qui n'écrivent pas par-dessus les programmes sont bien plus sournois que les précédents, car ils n'empiètent pas à priori sur le déroulement du programme-hôte, ce qui les rend encore plus difficiles à détecter.

Selon la classification de Steve Gibson, ce type de virus appartient également à la catégorie des virus universels (GPIV). Leur mécanisme de propagation fonctionne en règle générale sur le même principe que celui des virus écrivant par dessus les programmes. La principale différence réside dans la démarche d'accès au programme d'accueil.

Les mécanismes d'introduction des virus peuvent prendre des formes multiples, dont la plupart sont programmées avec intelligence, ce qui les rend extrêmement difficiles à cerner. Nous allons donc nous concentrer sur deux principes de base de leur fonctionnement :

Première variante



Lorsque le virus trouve un programme sain dans la mémoire de masse, il sélectionne au début de ce programme un nombre d'octets correspondant à sa taille plus l'espace nécessaire à son activité, et le place à la fin du programme.

Dans un second temps, le virus inscrit son code dans l'espace laissé vide au début du programme par le fragment transféré.

Chaque fois que le programme infecté est lancé, il contamine un programme sain de la façon décrite précédemment. Le virus rétablit le programme d'application manipulé qui se trouve dans la mémoire de travail en remettant le fragment déplacé à la fin, à son emplacement initial.

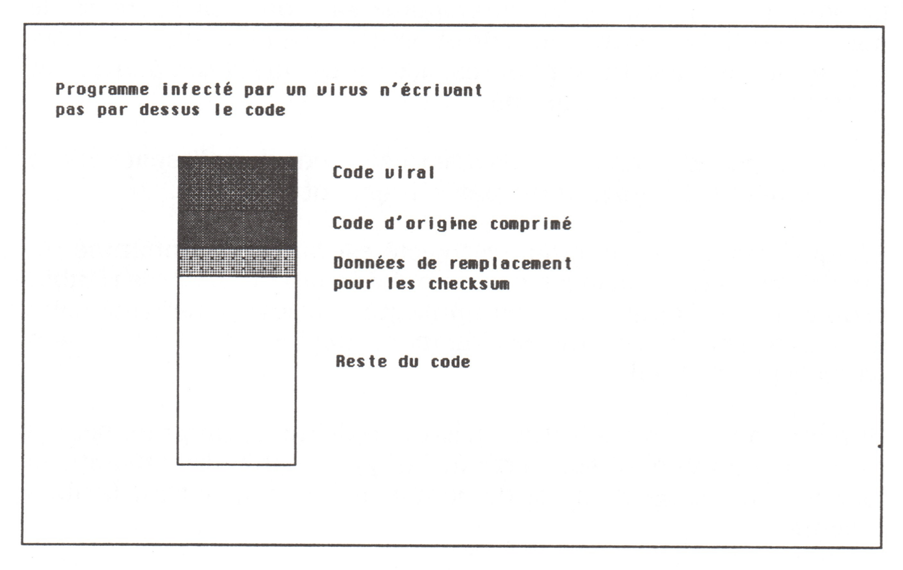
Et pour finir, le virus effectue un saut au début du programme, qui s'exécute maintenant sans erreur. Ce type de link-virus modifie la longueur du programme et de ce fait, il est relativement facile à repérer.

Seconde variante

Une autre variante des virus qui n'écrivent pas par-dessus les programmes pourrait se dérouler ainsi : tout d'abord, le virus calcule le ckecksum du programme à infecter. Puis il comprime un fragment de code qui se trouve au début du programme à l'aide d'une routine de compression (réduction du nombre d'octets).

Dans un second temps, le code viral s'inscrit devant le fragment comprimé pour combler l'espace libéré, de telle sorte que le ckecksum du code original ne présente de prime-abord aucune modification.

Lorsque le programme infecté est lancé, le virus est transmis au programme suivant de la façon décrite précédemment. Et pour finir, le virus rétablit le programme manipulé qui se trouve dans la mémoire de travail ; pour cela, il décomprime le fragment condensé du code original qui s'exécute comme si rien ne s'était produit.



Ce virus attaque tous les ordinateurs mais son action est particulièrement destructrice sur les systèmes équipés d'un disque dur. Le virus trahit sa présence en effectuant un certain nombre d'accès en écriture supplémentaires à chaque appel du programme, mais ce symptôme échappe le plus souvent à l'attention de l'utilisateur.

❒ 2.3. Virus résidents en mémoire

Les virus résidents en mémoire implantent leurs mécanismes de reproduction ou leurs tâches de manipulation dans les zones de mémoire qui ne sont pas effacées lors de l'initialisation de l'ordinateur. Les programmes ont la possibilité de protéger la zone de mémoire qu'ils utilisent pour empêcher le système d'exploitation de l'effacer lors d'une réinitialisation. Pour cela, la valeur de départ de la mémoire libre connue du système d'exploitation est augmentée en fonction de la taille du code viral.

Zone de mémoire

Mémoire de travail protégée

Mémoire de travail disponible

Mémoire totale

Mémoire de travail protégée

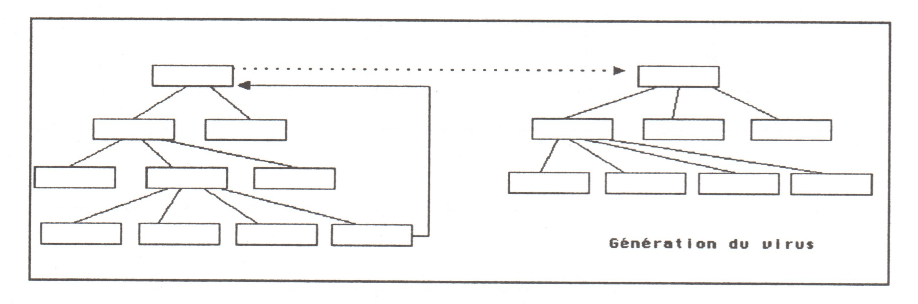
Code viral

Mémoire de travail disponible

Le virus s'accroche dans la structure d'interruption ou dans les variables système de l'ordinateur et agit même si le programme infecté n'a pas été lancé. Ce type de virus ne disparaît qu'après avoir complètement éteint l'ordinateur.

❐ 2.4. Virus évolutifs

Le virus évolutif modifie sa structure chaque fois qu'il se reproduit. Ainsi, chaque nouvelle génération de virus peut "hériter" une nouvelle tâche de manipulation ou se reconstituer au moment de la reproduction. Ce phénomène rend le processus de détection d'un virus reconnu auparavant extrêmement difficile, car le programme de recherche ne peut plus se fier à des critères stables.



S'il est programmé avec intelligence, ce type de virus capable d'évoluer de génération en génération, possède la faculté de réagir différemment sur chaque configuration. Les virus évolutifs sont dans une large mesure comparables aux link-virus.

❐ 2.5. Virus batch

Les virus batch sont des programmes conçus dans le langage de commande propre au système d'exploitation. Ils sont introduits sous forme de boot-virus ou en chaîne et peuvent réaliser les mêmes tâches.

❐ 2.6. Bactéries

En principe les bactéries ne sont rien d'autre que des virus. Leur nom provient probablement de leur spécificité : les bactéries visent tout particulièrement à paralyser le système en occupant progressivement l'ensemble de sa mémoire vive. Etant donné qu'ils ne possèdent en règle générale aucune autre tâche de manipulation, les bactéries sont très difficiles à identifier.

❐ 2.7. Chevaux de Troie

Les chevaux de Troie sont des programmes d'aide soi-disant utiles et dans la plupart des cas gratuits, portant des noms séduisants comme par exemple "SEXLADY.COM", ou "Porte-bonheur" et qui en dehors de leur fonction apparente réalisent un certain nombre d'opérations dissimulées et destructrices, sur une cible précise.

Le nom de "cheval de Troie" a été emprunté à la mythologie grecque. Pour ruser l'ennemi, Ulysse fit fabriquer un cheval de bois et se cacha avec quelques-uns de ses hommes dans le ventre du cheval pour pénétrer incognito dans la ville de Troie. Les chevaux de Troie informatiques ne se multiplient pas en règle générale.

Cependant, il est tout à fait possible de mettre au point un cheval de Troie qui, en plus de sa fonction d'introduire sournoisement un germe dans l'ordinateur, porterait en lui une tâche de manipulation destinée à le propager. Dans ce cas précis, le cheval de Troie agit comme un virus "père".

Dans cette optique, on pourrait dire que tous les programmes infectés par un virus sont en réalité des chevaux de Troie - à la vérité, le cheval de Troie n'est pas aussi inoffensif qu'il en a l'air - à condition toutefois de faire abstraction du point de vue sur la finalité d'un programme, que nous avons développé dans la définition des virus.

A l'heure actuelle, Il existe sur le marché de nombreux programmes connus sous le nom de "Brute Force" (Force Brutale) qui font des magnifiques chevaux de Troie. Pendant qu'un programme inoffensif en apparence se déroule au premier plan, ils s'affairent

tranquillement à reformater le disque dur ou à détruire les tables d'allocation de fichiers (FAT) qui contiennent les schémas d'organisation des données sur le disque dur.

La principale caractéristique de ces virus n'est pas de se multiplier, mais d'effectuer une manipulation aux conséquences immédiates à chaque lancement du programme. Les chevaux de Troie sont également utilisés pour subtiliser les mots de passe lorsque le programme est lancé par un utilisateur privilégié.

Une fois qu'il a accompli sa tâche, le programme efface automatiquement ses structures de manipulation pour brouiller les pistes. Une autre variante de ces "voleurs de mots de passe" consiste à espionner la procédure de connexion lors de laquelle l'utilisateur est appelé à entrer son mot de passe.

Pour se connecter sur un système UNIX, l'utilisateur doit entrer son nom suivi de son mot de passe. Certains programmes "espions" simulent la procédure de connexion normale et se déclenchent avant même que le système ne lance la procédure de connexion proprement dite.

C'est ainsi que l'utilisateur entre son nom et son mot de passe sans se douter de rien et s'étonne lorsque le système lui demande de recommencer sans envoyer les message d'erreurs habituels en cas de faute de frappe. Si cela arrive, modifiez votre mot de passe et prévenez l'opérateur dans les plus brefs délais.

❐ 2.8. Vers

Les vers sont des programmes qui ne se sont manifestés jusqu'à présent qu'à l'intérieur des réseaux. Ils prolifèrent également sur les lignes de transmission de données d'où ils transmettent une copie de leur code à chaque ordinateur. De façon générale, les vers ne peuvent pas être délogés par une simple réinitialisation du système et sont capables, tout comme les virus, de paralyser l'ensemble du système. Les dispositifs de sécurité intégrés aux logiciels de réseau présentent malheureusement encore des failles qui offrent une porte d'accès discrète à toutes sortes de "hackers" et de "crashers".

Les "hackers" laissent derrière eux un certain nombre de programmes dans le style des chevaux de Troie pour intercepter les mots de passe des utilisateurs et avancer ainsi progressivement dans la hiérarchie des droits d'accès. Lorsqu'un tel programme atteint le niveau de privilèges de l'opérateur chargé de contrôler le réseau, il crée un compte qui lui permettra d'accéder tout à fait normalement au système par la suite, au moyen d'une simple ligne téléphonique.

Les "crashers" procèdent de façon similaire, mais à la différence que les "vers" qu'ils introduisent se contentent d'agir à l'intérieur du réseau dans l'objectif de détruire les disques durs et de supprimer les comptes utilisateur. Les vers peuvent se glisser dans le réseau interne d'une entreprise et de là, passer dans toutes les sphères d'un système, multiplier leurs branches (sans toutefois infecter les programmes, comme le font les virus) et pousser les utilisateurs au bord de la crise de nerfs par toutes sortes d'affichages.

Chapitre 3

Les virus Atari

Cet ouvrage est accompagné de VIRtuel, qui est un logiciel de protection contre les virus spécialement conçu pour Atari ST. Nous allons donc examiner de plus près les virus les plus connus qui sévissent actuellement sur les systèmes Atari ST. Voici la liste des principaux virus Atari :

Type	Nom, action	Effets
Boot-virus	Attend une copie piratée d'Aladin pour se déclencher	Détruit Aladin
Boot-virus	Le virus "Mad" est activé toutes les 5 copies	Bip, intervertit l'écran
Boot-virus	Déclenché par la date système 1987	Détruit les tables d'allocation de fichiers (FAT) sur une disquette ou un disque dur
Boot-virus	Freeze, déclenché par les disquettes à 11 secteurs	Suspend les programmes en cours d'exécution
Boot-virus	Activé par les programmes GFA	Détruit les programmes GFA
Boot-virus	Déclenché par des programmes de type "Application Systems"	Détruit les programmes qui l'ont déclenché
Boot-virus	Déclenché lorsque la taille d'un fichier dépasse 100 Ko	Détruit les fichiers qui le déclenchent

Type	Nom, action	Effets
Boot-virus	Activé à la date du 31/12/1988	Détruit la tête de lecture du disque dur
Link-virus	"Bacille du charbon", activé par l'infection d'un programme	Détruit les tables d'allocation (FAT) de la disquette
Link-virus	VCS ; les conditions de déclenchement sont librement programmables	Librement programmable
Link-virus	Virus spécialement conçu pour 1st Word ; il se déclenche par hasard	Détruit les fichiers de texte
Link-virus	Modifie tous les fichiers ; activé tous les 7 lancements programme	Défaillance générale

Le virus Aladin

Au moment de lancer le programme de traitement de texte MacWrite sous Aladin, le système d'exploitation parallèle de l'Atari ST, l'image se met à défiler et s'arrête sur un nouvel en-tête portant le message suivant : "Frankie says: this is the end of piracy", après quoi, plus rien ne fonctionne.

Le MicroVirus

Le MicroVirus provoque l'arrêt de l'écran au bout de 180 minutes. Après la réinitialisation du système, l'image est reconstituée mais disparaît aussitôt.

Cette liste n'est pas exhaustive car MicroVirus possède à l'heure actuelle un nombre considérable de variantes qui se multiplieront sans doute à l'avenir. Il existe en R.F.A. un programme, "Virus-Construction-Set", permettant de mettre au point les virus les plus pervers sur l'Atari ST. Avec ce programme, l'auteur du virus peut faire des nombreuses victimes parmi les utilisateurs d'Atari sans même savoir programmer.

Piloté par menu, ce programme permet de "bricoler" des virus selon l'imagination de chacun, sans la moindre connaissance en matière de programmation, et offre de multiples options permettant de composer les virus les plus variés. Ce programme offre la possibilité

de produire des virus en série en modifiant au choix leur apparence, les stratégies d'infection et de manipulation de programmes et la fréquence de contamination.

Ce programme est à l'origine d'un nombre considérable de virus identifiés sur les systèmes Atari ST. La liste précédente répertorie les virus qui ont été développés à partir de ce kit. Les utilisateurs disposent ainsi d'un moyen pour provoquer d'importants dégâts avec des conséquences tout à fait imprévisibles.

Une fois en circulation, l'utilisateur n'a plus aucune possibilité de contrôler son virus. Pour cette raison, le "Virus-Construction-Set" est accompagné d'un antidote capable de détecter les logiciels infectés et de détruire le virus. Malheur à celui qui ne possède pas l'antivirus correspondant.

❐ 3.1. Les virus du boot-secteur

Le virus du boot-secteur attaque tous les ordinateurs qui possèdent la faculté de modifier leur système d'exploitation à chaque initialisation. Nous allons analyser l'action de cette espèce de virus sur l'Atari ST.

Le virus du boot-secteur doit son nom à son lieu de résidence sur la disquette à partir duquel il se fraye un chemin vers la mémoire centrale de l'ordinateur. Le boot-secteur est une zone fixe utilisée par le système d'exploitation pour y déposer les données associées à un programme spécifique ou pour lancer un programme à partir de la disquette.

Le boot-secteur a pour fonction de charger le système d'exploitation, MS-DOS par exemple, automatiquement, à partir de la disquette. Etant donné qu'il est limité en règle générale à 512 octets, le boot-secteur n'abrite pas l'ensemble du système d'exploitation, mais seulement un petit programme chargé de copier le système d'exploitation stocké sur la disquette dans la mémoire de travail.

Piste 1

Piste 2

Secteur 0

Secteur 1

```
Desk  Modify  Sector  Attributes

0000:  60 38 00 00 00 00 4E 4E-85 8A 2A 00 02 02 01 00  `8....NN..*.....
0010:  02 70 00 D0 02 F8 05 00-09 00 01 00 00 00 4E 4E  .p............NN
0020:  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0030:  4E 4E 4E 4E 4E 4E 4E 4E-00 00 41 FA FF C4 22 79  NNNNNNNN..A..."y
0040:  00 00 04 C6 D3 FC 00 00-06 00 24 49 30 3C 01 00  ..........$I0<..
0050:  32 D8 53 40 6A FA 41 FA-00 0C 43 FA FF A4 91 C9  2.S@j.A...C.....
0060:  D5 C8 4E D2 41 FA 00 C6-20 B9 00 00 04 72 41 FA  ..N.A... ....rA.
0070:  00 0A 23 C8 00 00 04 72-4E 75 4E 56 00 00 3F 2E  ..#....rNuNV..?.
0080:  00 08 20 7A 00 A8 4E 90-54 8F 48 E7 80 C0 41 FA  .. z..N.T.H...A.
0090:  00 A0 4A 50 67 00 00 8E-20 79 00 00 04 C6 30 10  ..JPg... y....0.
00A0:  B0 7C 60 38 67 5E 43 FA-FF 58 30 D9 30 D9 30 D9  .|`8g^C..X0.0.0.
00B0:  D3 FC 00 00 00 32 D1 FC-00 00 00 32 30 3C 00 E7  .....2.....20<..
00C0:  30 D9 53 40 66 FA 3F 3C-00 01 3F 3C FF FF 2F 3C  0.S@f.?<..?<../<
00D0:  FF FF FF FF 2F 39 00 00-04 C6 3F 3C 00 12 4E 4E  ..../9....?<..NN
00E0:  3F 3C 00 01 42 A7 3F 3C-00 01 3F 2E 00 08 42 A7  ?<..B.?<..?...B.
00F0:  2F 39 00 00 04 C6 3F 3C-00 09 4E 4E DF FC 00 00  /9....?<..NN....

Cursor at 0000: Hex=60  Bin=01100000  Dec=096  Asc=`

Track:  00                    Search   Continue
Drive: A
Sector: 01                    Relative Exit
```

Les boot-virus se sont massivement répandus sur les systèmes Atari ST pour différentes raisons :

Au début, l'Atari ST chargeait le système d'exploitation à partir d'une disquette. Pour cette raison, le boot-secteur de la disquette devait être prêt pour l'exécution à tout moment. Plus tard, on a intégré le système d'exploitation (TOS ou GEM) à l'ordinateur ; de ce fait, le boot-secteur n'était utilisé que par certains jeux. En dépit de ces modifications, l'Atari vérifie toujours, au moment de sa mise en route, si le lecteur A: contient une disquette avec un boot-secteur exécutable.

Cependant, le boot-secteur peut abriter un virus qui guette le moment où la disquette sera introduite dans le lecteur A: pour démarrer le système. Ce n'est qu'à partir de ce moment qu'il pourra entrer en action pour se multiplier et éventuellement exécuter une tâche de manipulation. Une fois lancé, le virus se glisse dans la mémoire de l'ordinateur, d'où il transmettra son code à toutes les disquettes saines placées dans le lecteur A:.

Pour cela, il "déforme" en quelque sorte les pointeurs dirigés habituellement sur les fonctions d'écriture et de lecture usuelles utilisés par le système d'exploitation TOS d'Atari pour localiser certaines fonctions, en introduisant des pointeurs sur ses propres routines.

Selon le pointeur "dévié", les routines manipulées par le virus peuvent déposer le code viral dans le boot-secteur de toutes les nouvelles disquettes, à chaque accès en lecture ou en écriture, ou alors exécuter une tâche de manipulation pré-définie, avant de réaliser l'opération attendue par le système d'exploitation.

L'aspect le plus dangereux de la plupart des boot-virus réside dans leur faculté de détruire, le cas échéant, les secteurs d'auto-initialisation utilisés pour certains programmes de loisirs ou pour démarrer un système d'exploitation parallèle. Le virus peut parfois se multiplier au moment même où vous consultez l'index de la disquette.

Certains virus ne disparaissent pas après la réinitialisation du système (virus résidents en mémoire). Pour les déloger, il faudrait éteindre l'ordinateur. Une simple pression sur la touche Reset ne

suffit pas pour les faire disparaître. Dans certains cas, le système Atari ST doit rester éteint pendant au moins 20 secondes pour que la mémoire soit entièrement effacée.

En cas d'apparition de boot-virus, nous vous conseillons de vérifier et, si nécessaire, restaurer et immuniser toutes vos disquettes à l'aide d'un programme de protection, comme par exemple VIRtuel pour Atari ST, que vous trouverez à la fin de ce livre.

❐ 3.2. Les link-virus

Les link-virus qui touchent aux systèmes Atari fonctionnent sur le principe que nous avons exposé sous 2.2. Certaines variantes plus récentes de ce virus déposent leur code dans une zone inutilisée de la mémoire de masse, comme par exemple, un segment de programme qui se trouve sur la piste 80 des disquettes Atari, ou dans la deuxième table d'allocation (FAT). Ce type de virus n'est pas très répandu sur Atari ST, car il est plus difficile à programmer que les boot-virus.

❐ 3.2.1. Le "bacille du charbon"

La publication du "bacille du charbon" sous forme de listing dans un magazine spécialisé a déclenché une épidémie à grande échelle. Ce virus a permis de mettre en circulation les variantes les plus diversifiées. Lorsqu'il est activé, le "bacille du charbon" vérifie tout d'abord la date du jour ; si celle-ci correspond à sa tâche de manipulation, il détruit irréversiblement tous les fichiers stockés sur les disquettes, quel que soit le lecteur utilisé.

Si les conditions de son déclenchement sont réunies, le virus écrit son code par dessus les premiers secteurs de la disquette, qui sous TOS abritent le répertoire système et les tables d'allocation (FAT). Il est pratiquement impossible de rétablir un répertoire détruit. Si la date du jour ne correspond pas, le virus cherche dans l'index de la disquette en cours un fichier .PRG dont la taille dépasse 10000 octets.

Le virus vérifie la taille du fichier pour ne pas être détecté prématurement. La modification de ce paramètre est plus facile à

détecter sur les petits que sur les gros fichiers. Lorsque le virus trouve un fichier qui réunit ces conditions, il vérifie dans un second temps si le programme n'a pas déjà été infecté.

Le processus d'infection consiste à déplacer les premiers octets du programme à la fin, en exécutant une instruction de saut, et à intégrer le code viral dans l'espace libéré. Lorsque le programme infecté est relancé à un moment ultérieur, la partie virale s'exécute en premier grâce à l'instruction de saut. Le programme infecté est ensuite rétabli dans son état initial, les adresses absolues sont corrigées et replacées au début. Le programme infecté se déroule à présent sans aucun incident. Deux autres variantes de ce virus ont été présentées dans la même publication.

❐ 3.2.2. Le virus VCS

Les virus VCS sont développés à partir du kit "Virus-Construction-Set" (VCS).

Chapitre 4

Le programme VIRtuel

❐ 4.1. Conditions requises

Le programme VIRtuel fonctionne sur tous les ordinateurs Atari ST avec le TOS en mémoire morte (ROM) et qui disposent d'au moins un lecteur de disquettes. Il ne s'adapte pas sur les systèmes Atari qui chargent le système d'exploitation TOS à partir d'une disquette. VIRtuel requiert environ 100 Ko de mémoire.

❐ 4.2. Connaissances préalables

Pour travailler avec VIRtuel, vous devez connaître les fonctions de base de l'ordinateur Atari ST : l'utilisation de Desktop et de la souris, le choix d'options sur la barre des menus, la sélection de fichiers dans les boîtes de dialogue, les méthodes de suppression et de copie de fichiers, etc...

Si vous n'êtes pas familiers avec ces fonctions, nous vous conseillons d'apprendre à les utiliser avant d'aborder le programme VIRtuel. Pour vous aider, consultez le manuel d'utilisation livré avec votre système, le livre "Bien débuter Atari ST, STE" édité par Micro Application et les annexes de ce livre qui vous fourniront toutes les informations nécessaires.

Les chapitres précédents vous offrent un bref aperçu du fonctionnement des boot-virus et des link-virus. Lisez ces chapitres avant d'aborder l'utilisation du programme VIRtuel.

❐ 4.3. Fonctionnement du programme VIRtuel

Ce chapitre constitue une introduction au programme VIRtuel. Ce logiciel met à la disposition de l'utilisateur, débutant ou expérimenté, un outil facile à utiliser pour détecter tous les virus, anciens et nouveaux.

VIRtuel a pour fonction de reconnaître et de signaler toutes les modifications provoquées par l'action des virus à l'intérieur d'un logiciel, d'une disquette ou sur le système d'exploitation de l'Atari ST que nous avons exposées dans les chapitres précédents. Si les modifications enregistrées ont été provoquées par un virus connu, VIRtuel vous communiquera également le type de virus incriminé. Le programme VIRtuel est capable de détecter les manipulations suivantes :

- Modification de la taille du programme
- Modification de la date de création du programme
- Modification des attributs d'un fichier
- Suppression d'un logiciel
- Apparition d'un nouveau logiciel
- Modification de la checksum
- Programme infecté par le "bacille du charbon"
- Programme infecté par un virus VCS
- Boot-secteurs exécutables
- Boot-secteurs infectés par un virus connu
- Protection du bootsecteur contre les virus

Pour détecter des virus à l'aide du programme VIRtuel, l'utilisateur n'est pas censé connaître la programmation de son système jusque dans les moindres détails ni même la structure spécifique de chaque virus.

Il doit pouvoir travailler sur son ordinateur comme d'habitude sans se soucier outre mesure de toutes ces choses désagréables que sont

les virus informatiques et en même temps, savoir se protéger au mieux contre les risques d'infection.

Dans ce contexte, la principale fonction de VIRtuel est d'informer l'utilisateur sur les changements inhabituels qui interviennent dans le fonctionnement de son logiciel et de lui proposer des mesures rationnelles. Les pages qui suivent présentent un bref aperçu du fonctionnement de VIRtuel. Le programme VIRtuel est composé de deux éléments qui remplissent des fonctions bien définies :

- T1.prg avec le fichier de ressources correspondant, T1.rsc
- T2.acc avec le fichier de ressources correspondant, T2.rsc

La section 4.5 présente une analyse détaillée du fonctionnement de ces deux programmes. VIRtuel T1.prg examine vos disquettes et votre disque dur en vue de détecter d'éventuels virus. Cette opération permet d'identifier tous les virus du bootsecteur et en chaîne connus à l'heure actuelle.

Pour détecter les virus qui ne sont pas encore connus, VIRtuel T1.prg vous offre la possibilité de tester vos disquettes et disques durs. Pour vous permettre d'établir un diagnostic, VIRtuel T1.prg conserve les principales caractéristiques de tous les programmes stockés sur une disquette ou un disque dur dans un fichier de texte spécifique. A chaque demande, le programme se charge de comparer ce fichier avec l'original et de vous signaler les changements qui ont eu lieu.

VIRtuel T1.prg vous offre d'autre part la possibilité d'archiver les bootsecteurs de vos disquettes pour vous permettre de rétablir les disquettes manipulées par des virus en cas de besoin. De plus, VIRtuel T1.prg établit une liste de logiciels qui sera utilisée par T2.acc pour effectuer des "petits" diagnostics tout au long de votre session de travail. De cette façon, les programmes sélectionnés seront automatiquement soumis à un examen minutieux en vue de détecter d'éventuels changements, sans aucune intervention de votre part.

L'accessoire de bureau VIRtuel T2.acc teste automatiquement jusqu'à 30 logiciels pendant votre session de travail, pour détecter d'éventuelles manipulations ou la présence d'un virus. Cette

opération est réalisée à l'aide d'une liste de logiciels établie au préalable par T1.prg. Par ailleurs, T2.acc permet de détecter les modifications subies par les variables système. La section suivante sera consacrée à l'installation des programmes T1.prg et T2.acc. Les fonctions et l'utilisation de VIRtuel seront décrites dans la section 4.5.

❐ 4.4. Installation de VIRtuel

Avant d'installer VIRtuel, vous devez effectuer une copie de travail et mettre l'original dans un lieu sûr, à l'abri de la poussière, de l'humidité et de l'électricité. Pour cela, copiez la disquette dans son intégralité et pas seulement les fichiers qu'elle contient.

❐ 4.4.1. T1.prg

Vous pouvez soit conserver les fichiers T1.prg, T1.rsc et VIRtuel.dat sur votre disquette de travail, soit les copier dans un dossier de votre choix sur une autre disquette ou sur le disque dur. Nous vous conseillons toutefois de les joindre à d'autres logiciels, comme par exemple un contrôleur de disques ou un éditeur de textes, que vous désirez lancer à partir de T1.prg.

A partir de VIRtuel T1.prg vous pouvez démarrer uniquement les programmes GEM qui se trouvent dans le même dossier. Si vous travaillez avec des disquettes, vous n'avez pas besoin d'effectuer d'autres installations. Lorsqu'il est activé, VIRtuel T1.prg lit le fichier VIRtuel.dat qui contient des informations sur les bootsecteurs connus et inoffensifs. Ce fichier sera rappelé à chaque examen de ces secteurs pour faire une comparaison et identifier les secteurs exécutables.

Si T1.prg ne trouve pas le fichier VIRtuel.dat dans le même dossier, il affiche un message d'erreur. Par conséquent, veillez à toujours placer les fichiers VIRtuel.dat et T1.prg ensemble.

Lors d'un examen des bootsecteurs, T1.prg vous permet en outre d'ajouter un certain nombre de secteurs isolés qui ne figurent pas dans le fichier VIRtuel.dat, de façon à les classer parmi les secteurs

inoffensifs. La section 4.5.4 analyse la procédure permettant d'enregistrer les bootsecteurs isolés dans une série de fichiers.

Créez un nouveau dossier avec le nom de votre choix sur la disquette destinée à archiver les bootsecteurs isolés. La disquette d'origine contient un dossier appelé "Boots" que vous pouvez utiliser pour cela.

Si les programmes ont subi des modifications anormales, T1.prg génère plusieurs fichiers pour rendre compte des changements opérés. Par conséquent, si vous travaillez avec un disque dur, créez un second dossier, avec un nom de votre choix, sur la partition de boot pour y stocker plus tard les fichiers journal. Ceci vous donnera une meilleure vue d'ensemble et vous facilitera la gestion des fichiers.

La disquette originale contient un dossier appelé Aender, que vous pourrez utiliser pour cela. Si vous travaillez avec des disquettes, stockez les fichiers journal de façon systématique sur la disquette qui contient les logiciels à examiner. Nous allons analyser ceux générés par VIRtuel dans le chapitre 4.5.

❒ 4.4.2. T2.acc

VIRtuel T2.acc est un accessoire de bureau qui ne peut être activé qu'au moment de la mise en route ou de la réinitialisation du système. Pour qu'il fonctionne correctement, il doit se trouver, comme tous les autres accessoires de bureau, dans le dossier principal du lecteur d'initialisation par défaut. Si vous travaillez avec un disque dur, le lecteur par défaut est en règle générale représenté par le prompt C:\ ; si vous utilisez des disquettes, le lecteur par défaut est A:\.

Recherchez maintenant vos accessoires de bureau sur le disque dur ou la disquette d'initialisation et copiez T2.acc dans le même dossier. Rappelez-vous que l'Atari ne peut charger plus de 6 accessoires. A partir de ce moment, démarrez votre système à partir de la disquette qui contient le fichier T2.acc pour lui permettre d'examiner les variables système à des intervalles de temps réguliers. Cependant, les programmes ne seront examinés que si vous avez créé une liste de logiciels au préalable. Nous allons

analyser la démarche utilisée pour dresser la liste des logiciels dans la section 4.5.3.1.

Si vous considérez qu'il n'est plus utile de soumettre les logiciels à une vérification régulière, il vous suffit de supprimer le fichier .vir dans le répertoire principal. Les variables système continueront toutefois à être vérifiées. Si vous désirez annuler toute procédure de vérification, supprimez tout simplement T2.acc dans le répertoire principal.

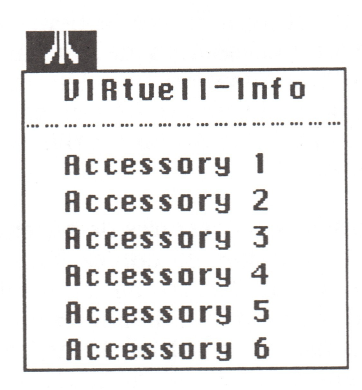
❐ 4.5. Le travail avec VIRtuel

❐ 4.5.1. Le menu et l'écran

Ce chapitre vous offre un bref aperçu des fonctions contenues dans les menus de T1.prg et de T2.acc. Après le lancement de VIRtuel T2.prg votre écran affiche une barre de menus et une boîte de dialogue. La barre de menus peut être utilisée de la façon habituelle et permet d'exécuter les fonctions suivantes :

Le menu Atari

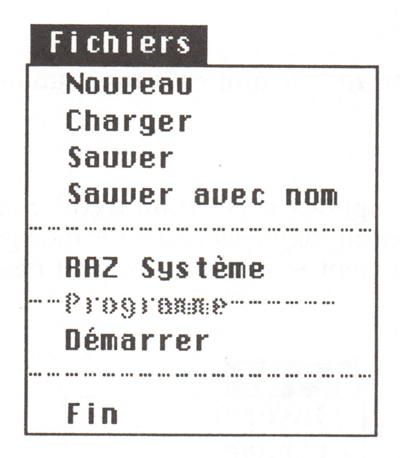
L'option "VIRtuel Info" affiche le Copyright et le numéro de version du programme.





Le menu Fichiers

Ce menu réunit les fonctions de chargement et d'enregistrement destinées aux listes de logiciels, les fonctions permettant de réinitialiser l'ordinateur, de lancer les programmes et de quitter le programme VIRtuel T1.prg



Nouveau

Cette option vous permet de créer une nouvelle liste de logiciels.

Charger

Cette option vous permet de charger la liste de logiciels valides.

Sauver, Sauver avec nom

Cette option vous permet d'enregistrer la liste de logiciels valides qui apparaît dans la boîte de dialogue sur disque.

RAZ Système

Sélectionnez cette option pour réinitialiser le système.

Démarrer

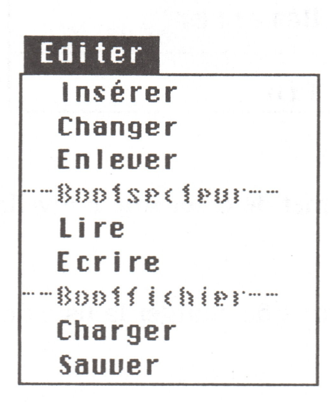
Cette option permet de lancer un programme extérieur, comme par exemple, un contrôleur de disques ou un éditeur de textes, sans pour cela quitter VIRtuel T1.prg. Si vous désirez activer un programme GEM à partir de T1.prg, vous devez le placer dans le même dossier, sinon, le système ne sera pas en mesure de localiser le fichier de ressources associé. Lorsque vous le quittez, vous retournez automatiquement dans T1.prg.

Fin

Cette option vous permet de quitter le programme VIRtuel.

Menu Editer

Ce menu réunit les options permettant d'éditer la liste de logiciels en cours, qui apparaît dans la boîte de dialogue ainsi que les fonctions de chargement et d'enregistrement des bootsecteurs de vos disquettes.



Insérer

Cette option vous permet d'insérer un nouveau programme dans la liste des logiciels pour le faire examiner.

Changer

Cette option vous permet de remplacer le programme qui apparaît dans la boîte de dialogue en vidéo inverse par un autre programme à l'intérieur de la liste des logiciels.

Enlever

Cette option permet de supprimer le programme qui apparaît dans la boîte de dialogue en vidéo inversée de la liste des logiciels.

Lire

Cette option est utilisée pour charger le bootsecteur de la disquette qui se trouve dans le lecteur A: ou B: dans la mémoire de travail et de l'examiner en vue de détecter d'éventuels virus. Si le programme détecte un virus, vous recevrez un message d'avertissement. Le bootsecteur de cette disquette reste dans la mémoire de travail jusqu'au moment où vous quittez VIRtuel ou exécutez les options "Charger", "Lire" ou le menu "Tester" qui effacent les valeurs en cours.

Ecrire

Cette option permet de copier le bootsecteur préalablement chargé dans la mémoire de l'ordinateur à l'aide des options "Lire", "Charger" ou du menu "Tester" sur la disquette qui se trouve dans le lecteur A: ou B:.

Charger

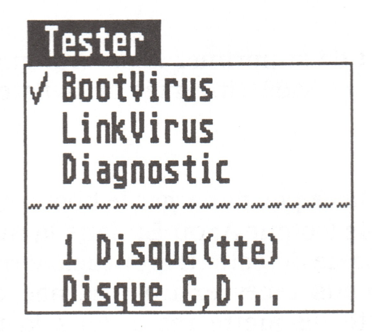
Cette option permet de charger un bootsecteur préalablement enregistré dans un fichier par la commande "Enregistrer". Le programme examine le bootsecteur chargé et s'il détecte un virus, il affiche un message d'avertissement. Le bootsecteur de cette disquette reste dans la mémoire de travail jusqu'au moment où vous quittez VIRtuel ou exécutez les options "Charger", "Lire" ou le menu "Tester" qui effacent les valeurs en cours.

Sauver

Cette option permet de sauver un bootsecteur préalablement chargé dans la mémoire de travail par les commandes Charger ou Lire, dans un fichier spécifique.

Le menu Tester

Ce menu réunit les options permettant d'examiner les disquettes, le disque dur et les logiciels.



Bootvirus

Cette option permet d'activer/désactiver la fonction de vérification portant sur les virus du bootsecteur.

LinkVirus

Cette option permet de d'activer/désactiver la fonction de vérification portant sur les link-virus.

Diagnostic

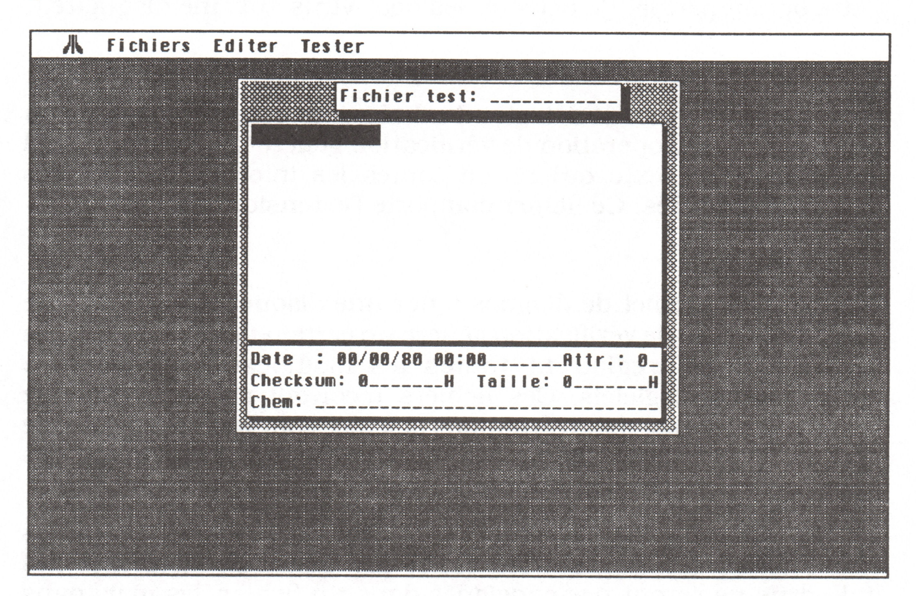
Cette option permet d'activer/désactiver le mode diagnostic.

1 Disque(tte)

Cette option permet d'examiner, en fonction des trois premières options (Boot-virus, Link-virus ou Diagnostic), une disquette ou un lecteur spécifié.

Disque C, D...

Cette option permet d'examiner, suivant la position des trois premières options, toutes les unités de disque spécifiées à partir de C. Lorsque vous lancez T1.prg, votre écran affiche une boîte de dialogue qui vous permet de dresser la liste des logiciels. Cette liste sera utilisée lors de la prochaine vérification automatique réalisée par VIRtuel T2.acc.



Si le programme VIRtuel T2.acc a été chargé lors de la mise en route de l'ordinateur, on pourra par le menu Atari accéder à VIRtuel T2.acc. Lorsque vous sélectionnez cette option, votre écran affiche une boîte de dialogue avec le copyright et l'intervalle de temps défini entre deux vérifications. Cette possibilité porte uniquement sur les programmes qui peuvent activer un accessoire ; T1.PRG n'en fait pas partie.

❐ 4.5.2. Vérification manuelle

Nous vous conseillons de vérifier systématiquement toutes vos disquettes neuves, celles que vous utilisez régulièrement et votre disque dur à l'aide de T1.prg pour détecter d'éventuels virus ou modifications anormales. Ceci implique une vérification manuelle

réalisée par le programme T1.prg sous l'option "Disquette et Disque du menu" Tester. Ce menu contient trois autres options qui déterminent, suivant la position sélectionnée pour les trois premières, le type d'examen à effectuer sur les disquettes ou disques durs.

Bootvirus

Cette option permet de détecter les boot-virus sur une disquette.

Linkvirus

Cette option permet de détecter des link-virus sur une disquette ou un disque dur. L'opération de vérification génère un fichier journal sous forme de texte qui réunit toutes les informations sur les link-virus détectés. Ce fichier comporte l'extension .lvs.

Diagnostic

Cette option permet de diagnostiquer une disquette ou un disque dur. L'opération de vérification génère un certain nombre de fichiers de texte qui enregistrent toutes les modifications opérées à l'intérieur des logiciels. Ces fichiers reçoivent en règle générale l'extension .cmp et .lst. Les options activées sont indiquées par une coche. Si plusieurs options sont activées simultanément, les fonctions correspondantes seront exécutées en parallèle.

Si les options "Diagnostic" et "Linkvirus" sont activées simultanément, les résultats de la procédure de détection des link-virus ne seront pas consignés dans un fichier .lvs mais dans les fichiers .cmp et .lst. Suivant les fonctions activées, vous devrez spécifier éventuellement les noms des fichiers destinés à enregistrer les résultats de la vérification. Nous allons maintenant approfondir et expliquer les différents messages d'avertissement.

❒ 4.5.2.1. Le dépistage des boot-virus

La vérification du bootsecteur porte uniquement sur les disquettes exécutables. Pour en détecter d'éventuels, procédez comme suit :

Première étape

Lancez T1.prg. Si le fichier VIRtuel.dat n'a pas été chargé, vous recevrez un message d'avertissement. Sélectionnez la case Annuler

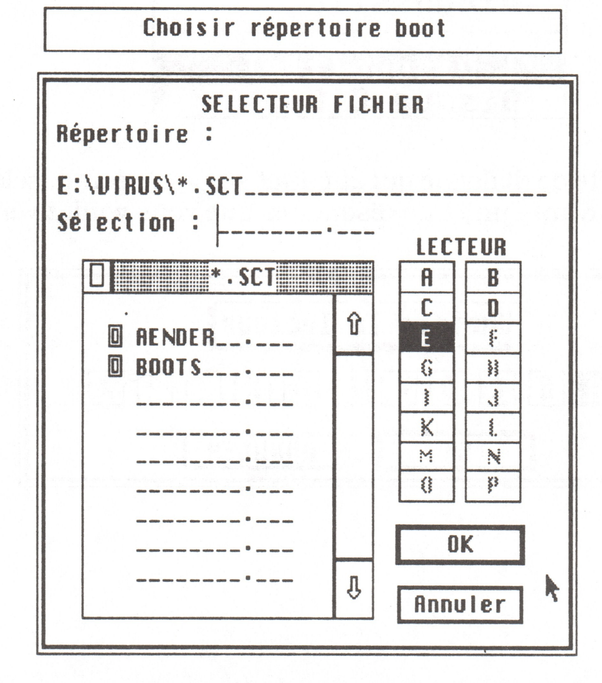
pour quitter le programme et copiez le fichier VIRtuel.dat dans le dossier ou se trouve T1.prg. Pour toutes informations complémentaires sur les messages d'avertissement, consultez la section 4.5.3.4.

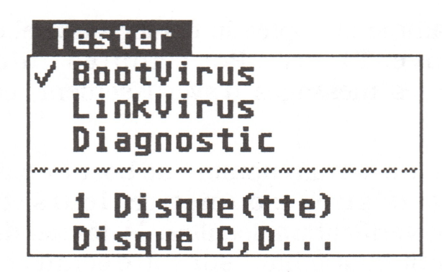
Si vous avez déjà réuni un certain nombre de bootsecteurs dans un dossier et si vous désirez soumettre leurs disquettes correspondantes à une vérification, localisez le dossier dans la boîte de sélection qui apparaît maintenant sur votre écran et cliquez sur la case OK pour confirmer.

Mais attention ! Ne mettez dans ce dossier que les bootsecteurs exécutables inoffensifs, car VIRtuel T1.prg part du principe que les fichiers stockés dans celui-ci sont inoffensifs. Si vous n'en avez pas encore constitué avec les bootsecteurs que vous désirez faire examiner, cliquez sur la case Annuler.

Deuxième étape

Activez l'option "Bootvirus" dans le menu Tester.

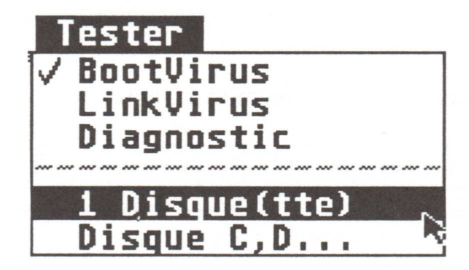




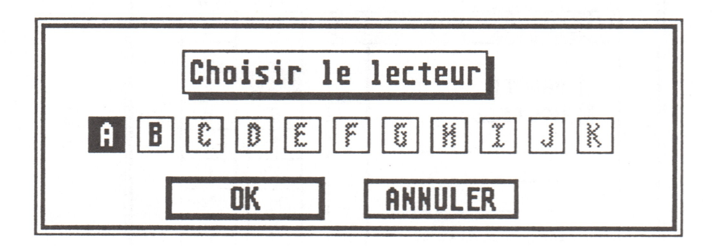
Pour notre exemple, désactivez toutes les autres options cochées.

Troisième étape

Sélectionnez maintenant l'option "1 Disque(tte)" dans le menu Tester.

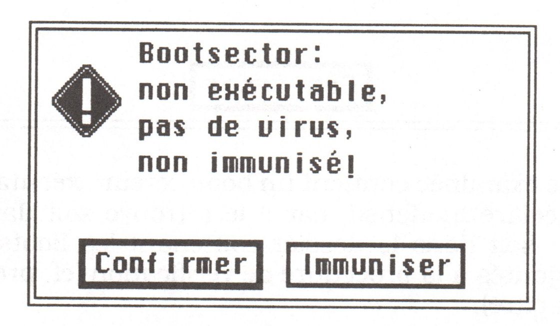


Dans la boîte de dialogue qui apparaît sur votre écran, sélectionnez A: ou B: suivant l'unité de disquettes que vous voulez vérifier.



Dans cette boîte de dialogue on ne peut activer qu'une seule option à la fois. Cliquez sur la case OK pour confirmer. Introduisez la disquette que vous désirez examiner dans le lecteur sélectionné. Le programme examine le bootsecteur et affiche les résultats dans une boîte de dialogue qui peut prendre différentes formes :

Première variante

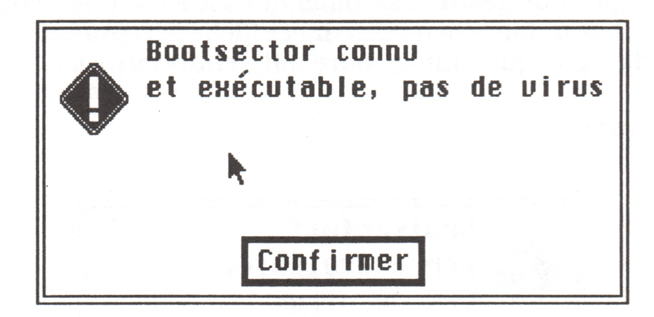


Le bootsecteur de la disquette ne contient aucun virus. Cependant, la disquette n'est pas immunisée, ce qui signifie qu'elle reste vulnérable. Pour éviter toute infection ultérieure, immunisez votre disquette en sélectionnant la case Immuniser.

Une fois cette opération accomplie, le bootsecteur inoffensif est enregistré sur la disquette. Tout bootsecteur exécutable produit un effet dissuasif sur tous les virus qui n'écrivent pas leur code dans un secteur exécutable.

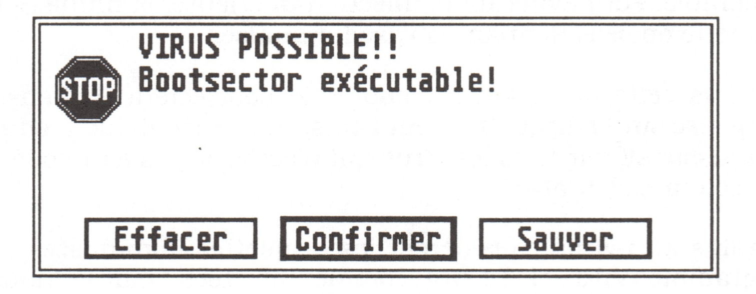
Certains anti-virus considèrent les disquettes immunisées par le programme VIRtuel T1.prg comme infectées, car le nouveau bootsecteur généré lors de cette opération reste malgré tout exécutable. Vous pouvez toutefois annuler la procédure de modification du bootsecteur en sélectionnant la case OK.

Deuxième variante



La disquette examinée contient un bootsecteur exécutable. VIRtuel T1.prg le déclare inoffensif, car il le retrouve soit dans le fichier VIRtuel.dat, soit dans le dossier contenant les bootsecteurs que vous avez ajoutés à la procédure de vérification (cf. première étape dans ce chapitre).

Troisième variante



Le bootsecteur de la disquette est exécutable, mais inconnu du programme VIRtuel T1.prg. Cela signifie que T1.prg n'a pas été en mesure de localiser le bootsecteur ni dans le fichier VIRtuel.dat, ni dans le dossier que vous avez spécifié. Par conséquent la présence d'un bootvirus reste possible.

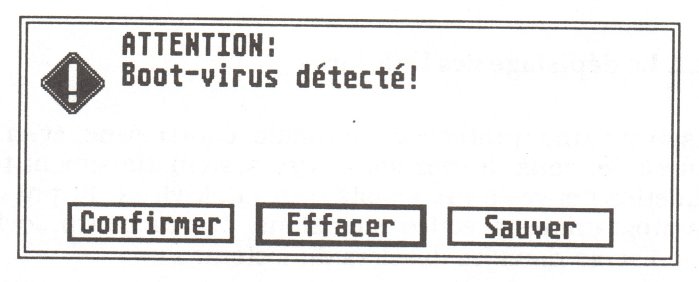
Vous avez trois possibilités : cliquer sur la case Sauver pour sauvegarder le bootsecteur dans un fichier afin de le ré-examiner ultérieurement, sélectionner la case Effacer pour l'effacer et en

même temps immuniser la disquette, ou alors annuler l'opération en choisissant la case Confirmer.

Pour éviter d'effacer par mégarde un bootsecteur dont vous auriez encore besoin (certains jeux nécessitent un bootsecteur spécial pour démarrer), sauvegardez-le dans un fichier en cliquant sur la case Enregistrer. Donnez-lui un nom évocateur avec l'extension .sct dans la boîte de sélection qui apparaît maintenant sur votre écran.

Vous pourriez charger ces fichiers à partir de VIRtuel T1.prg en vue de les remettre dans un bootsecteur.

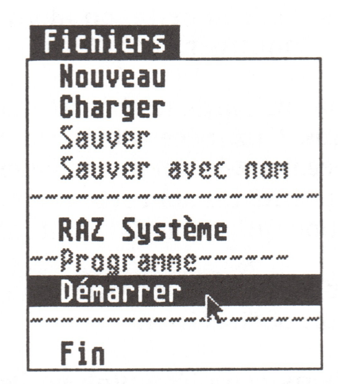
Pour toutes informations complémentaires, lisez les sections 6.1 et 6.3.



VIRtuel T1.prg a détecté un boot-virus connu sur la disquette. Pour le supprimer, cliquez sur la case Détruire. Si vous désirez faire examiner la disquette par un autre programme, cliquez sur la case Enregistrer pour sauvegarder le virus dans un fichier et spécifiez son nom dans la boîte de dialogue qui s'affiche maintenant sur votre écran.

Veillez à ne pas enregistrer ce fichier par inadvertance dans un bootsecteur sain, car cela permettrait au virus de se propager. La case Annuler vous permet d'ignorer l'avertissement qui s'affiche dans la boîte de dialogue, mais soyez extrêmement vigilants lorsque vous manipulez la disquette contaminée.

L'option "Demarrer" du menu Fichier vous offre également la possibilité de lancer un autre programme, un contrôleur de disquettes par exemple, pour connaître les fonctions exécutées par le bootsecteur examiné. Lorsque vous quittez le contrôleur de disquettes ou un autre programme activé par la commande "Mise en route", vous retournez automatiquement dans VIRtuel T1.prg.



Si vous désirez lancer un autre programme, spécifiez son nom dans la boîte de sélection.

❐ 4.5.2.2. Le dépistage des link-virus

Pour assurer une protection optimale contre une éventuelle infection virale, vous devriez soumettre systématiquement toutes vos disquettes neuves à un dépistage des link-virus. T1.prg vérifie tous les programmes avec les extensions .prg, .acc, .ttp, .ovl, .tos et .app, présents dans les dossiers du lecteur.

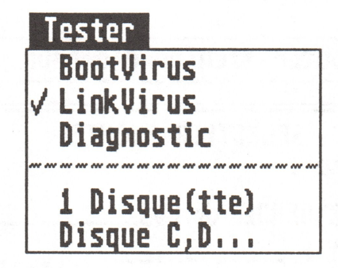
En cas d'infection par un link-virus recensé, vous recevrez un message d'avertissement. Toutes les informations concernant les programmes contaminés sont enregistrées dans un fichier de résultats avec l'extension .lvs. Pour soumettre les disquettes et disques durs à un dépistage des link-virus recensés, procédez de la façon suivante :

Première étape

Lancez T1.prg. Si le fichier VIRtuel.dat n'a pas été chargé, vous recevrez un message d'avertissement. Cliquez sur la case OK pour ignorer ce message car le fichier VIRtuel.dat ne participe pas au dépistage des link-virus. Dans la boîte de dialogue qui s'affiche maintenant sur votre écran, sélectionnez l'option Annuler car les bootsecteurs que vous avez éventuellement trouvés n'entrent absolument pas en ligne de compte lors d'un dépistage des link-virus.

Deuxième étape

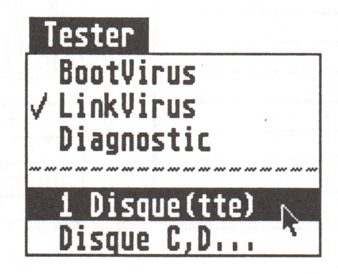
Cliquez l'option "Link-virus" dans le menu Tester.



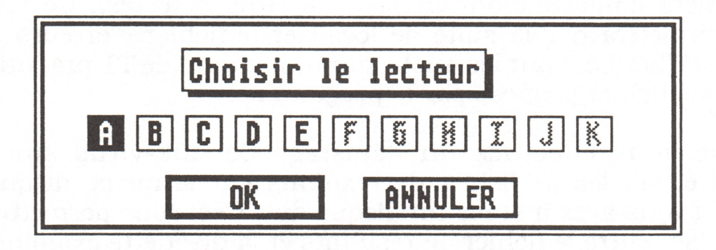
Pour cet exemple, désactivez toutes les autres options cochées.

Troisième étape

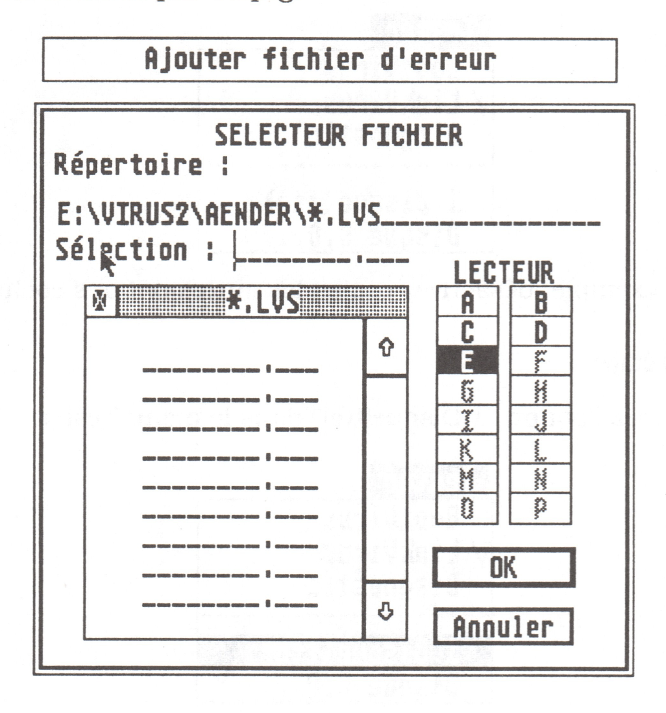
Sélectionnez l'option "1 Disque(tte)" dans le menu Tester.



Dans la boîte de dialogue qui apparaît sur votre écran, sélectionnez l'unité de disques(ttes) que vous désirez soumettre à une vérification.



Dans cette boîte, on ne peut activer qu'une seule option à la fois. Cliquez sur la case OK pour confirmer. Dans la boîte suivante, spécifiez le fichier de résultats qui recevra les informations sur les link-virus détectés par T1.prg.



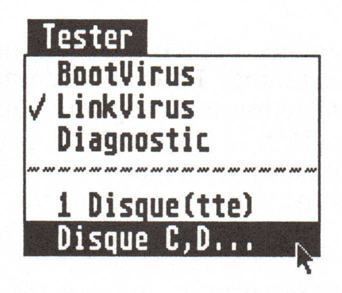
T1.prg vous propose un nom de fichier composé de la lettre L (qui représente le lecteur), suivie de son origine (par exemple A, B, C ou plus pour tous ceux examinés à partir du disque C) avec l'extension spécifique au type du fichier (dans ce cas, l'extension .lvs désigne les fichiers d'information sur les link-virus détectés). Ce format vous permettra par la suite de localiser le fichier d'erreurs sans aucune difficulté. Pour les applications standard de T1.prg, utilisez le nom de fichier proposé par le programme.

Lorsque vous effectuez un dépistage de link-virus sur une disquette, stockez le fichier de résultats sur la même disquette, même si vous avez installé un disque dur. Ceci vous permettra de faire le lien entre le fichier de résultats et la disquette examinée.

Lorsque vous examinez un disque dur, placez le fichier de résultats dans le dossier intitulé MODIF qui a été généré lors de l'installation de VIRtuel dans le répertoire principal du disque dur.

Cliquez sur la case OK pour confirmer votre choix. Comme nous l'avons déjà mentionné, T1.prg examine les programmes avec les extensions .prg, .acc, .ttp, .ovl, .tos, et .app placés dans les dossiers du lecteur spécifié.

Dans le menu Tester, vous pouvez sélectionner l'option "Disque C, D...", au lieu de "1 Disque(tte)", de façon à appliquer la procédure de dépistage sur tous les lecteurs déclarés à partir de C. Si votre système n'est pas équipé d'un disque dur ou d'un disque RAM, votre recherche portera uniquement sur les lecteurs A et B.



Quatrième étape

La procédure de dépistage de link-virus peut prendre un certain temps, suivant le nombre de programme présents sur le lecteur sélectionné. Une fois que tous les programmes ont été vérifiés, le résultat de l'examen s'affiche dans une boîte de dialogue :

Première variante



Le programme n'a détecté aucun link-virus

Le lecteur examiné ne contient aucun des link-virus connus. Le nombre des virus VCS et des "Pustules malignes" détectés est égal à 0.

Deuxième variante

Le programme a détecté des link-virus

Le message qui s'inscrit dans la boîte de dialogue indique que le nombre de link-virus détectés sur le lecteur examiné est supérieur à 0. T1.prg indique les logiciels infectés dans le fichier de résultats avec l'extension .lvs. Quittez T1.prg et consultez le fichier de résultats.

Cependant, le link-virus détecté a certainement eu le temps d'infecter votre programme. Pour le décontaminer, accédez au fichier journal en sélectionnant l'option "Ouvrir" dans le menu Fichier de l'application DESKTOP et procédez suivant les instructions fournies dans la section 5.3. Vous trouverez toutes les indications nécessaires pour interpréter ce fichier dans la section 4.7.

Ne lancez jamais un programme infecté car le virus pourrait se propager.

❒ 4.5.2.3. Etablir un diagnostic

Pour assurer un degré de protection optimal contre une éventuelle infection virale, vous devez diagnostiquer régulièrement toutes les nouvelles disquettes, celles que vous utilisez le plus souvent ainsi que votre disque dur. Dans un premier temps, nous allons vous présenter un bref aperçu de la méthode employée par T1.prg pour établir un diagnostic.

Dans un second temps, vous apprendrez comment faire exécuter un diagnostic. Tous les programmes .prg, .acc, .ttp, .ovl, .tos et .app figurant dans les dossiers du lecteur spécifié sont rassemblés et chargés successivement dans la mémoire de travail pour enregistrer les paramètres suivants : checksum, taille du fichier, date et heure de création, attributs.

En même temps, nous allons procéder à une vérification pour voir si l'un de ces programmes n'a pas été infecté par un link-virus. Les données rassemblées seront stockées dans un fichier portant l'extension .lst (LiST). Si le programme a détecté un link-virus, vous recevrez un message d'avertissement dans une boîte de dialogue. Tous les logiciels infectés seront marqués dans le fichier de résultats.

Si le dossier que vous avez spécifié sur ce lecteur contient déjà un fichier .lst, T1.prg suppose que le lecteur indiqué après la lettre L dans la spécification du fichier .lst a déjà été diagnostiqué. Le fichier journal établi lors du dernier diagnostic sur l'état du programme prend l'extension .bak (BAcKup) et sera comparé avec le nouveau fichier de résultats portant l'extension .lst.

Si le contenu de ces deux fichiers n'est pas identique, T1.prg affiche le résultat dans une boîte de dialogue et enregistre tous les points divergents dans un fichier de texte du même nom avec l'extension .cmp (CoMPare, comparer).

Si ce fichier ne figure pas dans le dossier spécifié, T1.prg suppose que le lecteur n'a jamais été diagnostiqué. Il n'effectuera aucun test et d'ailleurs, que pourrait-il examiner ?

Après cette brève incursion dans la démarche employée par T1.prg, nous allons voir comment se déroule le diagnostic. Pour établir un diagnostic, procédez comme suit :

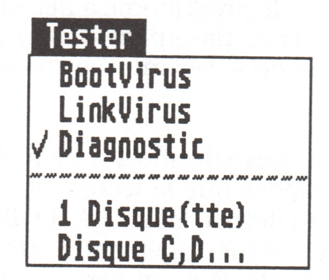
Première étape

Lancez T1.prg. Si le fichier VIRtuel.dat n'a pas été chargé, vous recevrez un message d'avertissement. Cliquez sur la case OK pour ignorer ce message, car le fichier VIRtuel.dat ne participe en aucune manière à la réalisation du diagnostic.

Dans la boîte de dialogue qui s'affiche maintenant sur votre écran, sélectionnez l'option Annuler car les bootsecteurs que vous avez éventuellement réunis n'entrent absolument pas en ligne de compte lors d'un diagnostic.

Deuxième étape

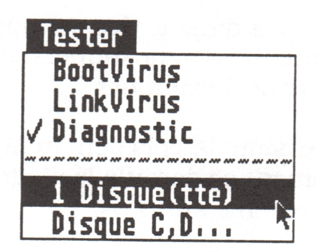
Cliquez l'option "Diagnostic" dans le menu Tester.



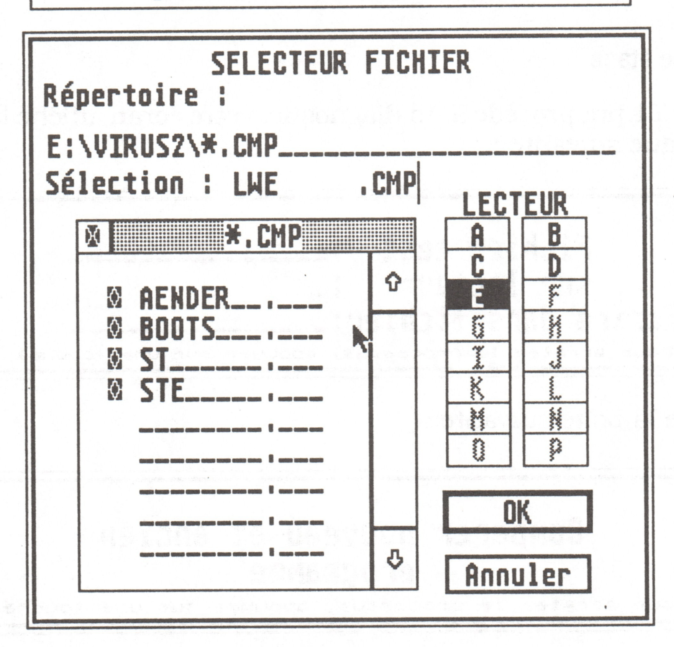
Pour les besoins de notre exemple, desactivez toutes les autres options cochées.

Troisième étape

Sélectionnez l'option "1 Disque(tte)" dans le menu Tester.



Dans la boîte de dialogue qui apparaît sur votre écran, sélectionnez le lecteur que vous désirez diagnostiquer. Dans cette boîte de dialogue.on ne peut activer qu'une seule option (lecteur) à la fois. Pour confirmer votre choix, cliquez sur la case OK. Dans la boîte suivante, spécifiez le fichier de résultats qui recevra les modifications de programmes détectées par T1.prg.



T1.prg vous propose un nom de fichier composé de la lettre L (qui représente le lecteur), suivie de la spécification du lecteur (par exemple A, B, C ou plus pour tous les lecteurs examinés à partir du disque C) avec l'extension spécifique au type de fichier de résultats (dans ce cas, l'extension .cmp désigne les fichiers qui contient les résultats du diagnostic). Pour les applications standard de T1.prg, utilisez le nom de fichier proposé par le programme.

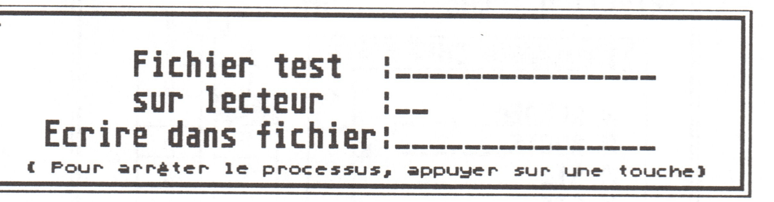
Lorsque le diagnostic porte sur une disquette, stockez le fichier de résultats sur la disquette examinée. De cette façon, vous pourrez facilement faire le lien entre le fichier de résultats et la disquette examinée. Lorsque vous examinez un disque dur, placez le fichier de résultats dans le dossier MODIF généré lors de l'installation de VIRtuel.

Cliquez sur la case OK pour confirmer votre choix. Dans le menu Tester, vous pouvez sélectionner l'option "Disque C,D...", au lieu de

"1 Disque(tte)", pour faire examiner l'ensemble des lecteurs déclarés à partir de C.

Quatrième étape

Lorsque T1.prg procède à un diagnostic, votre écran affiche la boîte de dialogue suivante :



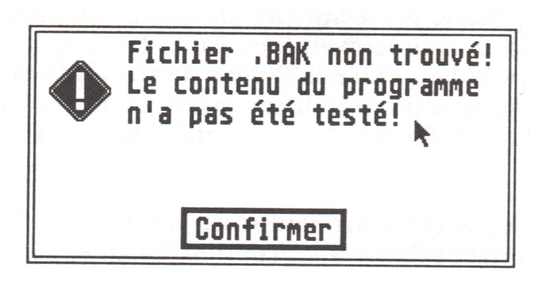
suivie de la boîte suivante :

Comparer nouveau et ancien programme

(Pour arrêter le processus, appuyer sur une touche)

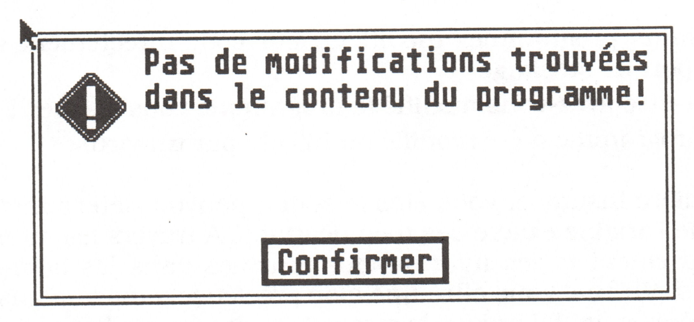
La procédure de diagnostic peut prendre un certain temps, suivant le nombre de programmes présents sur le lecteur sélectionné et en particulier s'il s'agit d'un disque dur. Une fois que tous les programmes ont été vérifiés, vous recevrez le résultat du diagnostic dans une boîte de dialogue :

Première variante



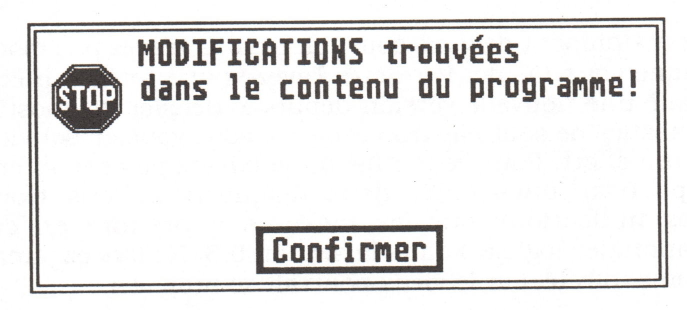
Ce message indique qu'aucun diagnostic n'a été établi étant donné qu'il n'y avait aucun fichier Lx.lst sur l'état précédent des programmes enregistrés sur le lecteur spécifié. Ce fichier est absolument indispensable pour effectuer la comparaison. Cette tentative de diagnostic génère un nouveau fichier .lst pour y stocker l'index et l'état des programmes enregistrés sur le lecteur spécifié. Ce fichier servira de base de comparaison lors du prochain diagnostic.

Deuxième variante



Ce message indique que l'état des programmes enregistrés sur le lecteur spécifié n'a pas été modifié depuis le dernier diagnostic. Aucun programme n'a été supprimé ou intégré dans la liste. Si les programmes étaient sains au moment du dernier diagnostic, il est fort probable qu'ils le soient toujours. Mais s'ils étaient déjà infectés par un virus inconnu ayant échappé à T1.prg, il ne se sont pas propagés car la procédure de diagnostic repère la moindre modification opérée sur le contenu des programmes.

Troisième variante



Le diagnostic révèle les modifications suivantes sur un ou plusieurs programmes :

- Suppression d'un ou plusieurs logiciels
- Apparition de nouveaux logiciels
- Modification des paramètres suivants : checksum, taille du fichier, date de création et attributs du fichier.

Ces modification peuvent avoir différentes origines :

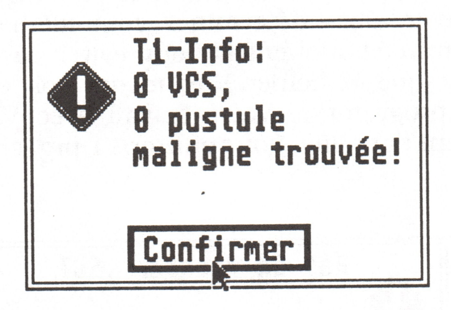
- Certains programmes modifient leur code directement sur le support de stockage
- Peut-être avez-vous modifié le programme vous-même ?!
- Le programme a été modifié ou infecté par un virus

En dernière instance, vous êtes le seul à pouvoir déterminer avec certitude l'origine exacte des modifications. A travers les messages d'avertissement et les informations fournies dans les fichiers de résultats, VIRtuel vous offre une aide précieuse dans la réalisation du diagnostic final. Lorsque le message ci-dessus s'affiche sur votre écran, consultez le fichier de résultats généré par T1.prg, sous le nom LWx.cmp pour savoir quels logiciels ont été modifiés et de quelle façon.

Quittez T1.prg. Votre programme a certainement été infecté par le link-virus détecté. Pour le décontaminer, accédez au fichier journal en sélectionnant l'option "Ouvrir" dans le menu Fichier de DESKTOP. Ce fichier conserve la liste de tous les logiciels modifiés. Vous trouverez toutes les indications nécessaires pour interpréter ce fichier de résultats dans la section 4.7.

Essayez maintenant de vous souvenir si vous n'avez pas modifié le programme vous-même. Peut-être l'avez-vous protégé en écriture ou installé une nouvelle version depuis le dernier diagnostic ? Si les diagnostics ne sont pas trop espacés, vous vous en souviendrez sans grand effort. Pour cette raison, ne laissez pas des intervalles de temps trop longs entre deux diagnostics. Vous trouverez quelques indications sur les mesures à prendre en cas de modification des logiciels dans la section 5.3. Ne lancez jamais un programme infecté, car le virus pourrait se propager.

Quatrième variante



Message sur les link-virus

Le message qui s'inscrit dans la boîte de dialogue après le diagnostic indique le nombre des link-virus détectés. Si le diagnostic a signalé la présence de link-virus, les logiciels contaminés seront marqués dans le fichier de résultats généré par la procédure de diagnostic. Pour plus de précisions, relisez la section 4.5.2.2. La section 5.3. explique comment agir en cas d'infection par un link-virus.

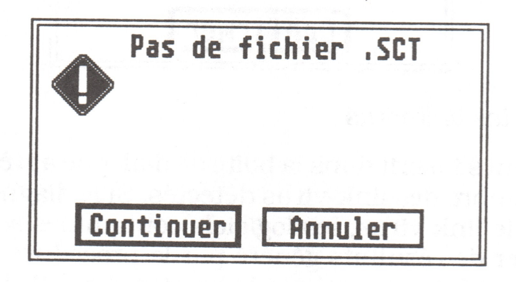
❐ 4.5.2.4. Messages d'avertissement

Les messages d'avertissement émis par T1.prg sont destinés à vous informer lorsqu'une fonction n'a pas pû être exécutée.

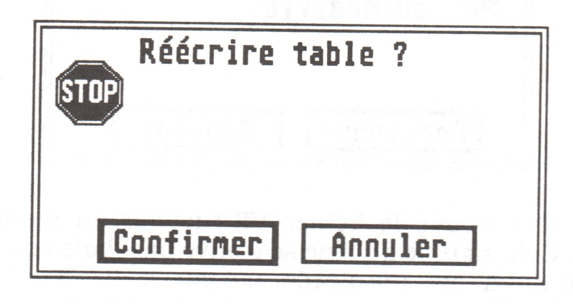


T1.prg n'a pas trouvé le fichier VIRtuel.dat au moment de son lancement. Cela signifie qu'il ne se trouve pas dans le même dossier ou alors qu'il a été manipulé illégalement. Pour annuler la procédure de comparaison avec les bootsecteurs connus, cliquez sur la case OK.

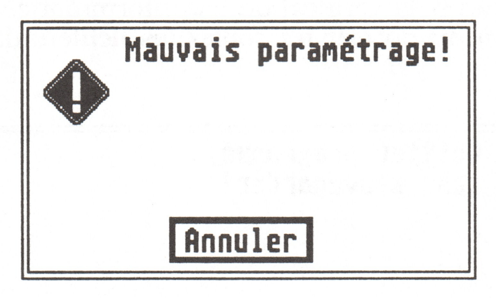
Cependant, la procédure de test des bootsecteurs exécutables génère un message pour vous signaler la présence éventuelle d'un virus. Vous devez alors déterminer vous-même s'il s'agit d'un bootsecteur connu et inoffensif. Pour éviter ce détour, faites le nécessaire pour que le fichier VIRtuel.dat soit chargé à chaque lancement du programme. Votre travail avec VIRtuel en serait considérablement simplifié. Pour quitter T1.prg, cliquez sur la case Annuler.



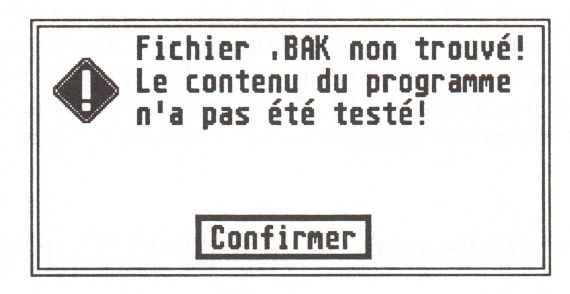
T1.prg vous informe que le répertoire principal sélectionné ne contient aucun fichier .sct (bootsecteurs). Si vous avez réuni, parallèlement à VIRtuel.dat, un certain nombre de bootsecteurs pour les soumettre à la test et si vous désirez les faire charger par T1.prg, cliquez sur la case Annuler pour quitter le programme, puis relancez T1.prg en spécifiant le répertoire principal correspondant dans la boîte de dialogue. Si vous n'avez pas encore constitué un dossier avec les bootsecteurs isolés ou si vous ne désirez pas les utiliser, sélectionnez la case Continuer pour poursuivre votre travail avec T1.prg.



Lorsque vous chargez ou remaniez une liste de logiciels (Teste.vir), T1.prg vous met en garde pour éviter un effacement involontaire de la liste de logiciels active.

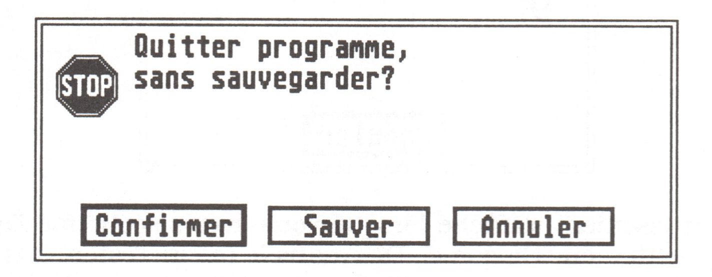


Cet avertissement s'affiche lorsque vous avez sélectionné l'option "1 Disque(tte)" ou "Disque C, D..." dans le menu Tester sans avoir coché aucune des trois premières options (Boot-virus, Link-virus ou Diagnostic) au préalable, ou lorsque vous avez activé uniquement l'option "Boot-virus" pour vérifier le disque dur.



Cet avertissement apparaît lorsque la liste établie au moment du dernier diagnostic sur le lecteur spécifié est introuvable. Par conséquent, la comparaison ne peut pas avoir lieu.

VIRtuel n'accepte pas le caractère "_" (Erreur TOS) dans la spécification du dossier sur le lecteur A: ou B:. S'il trouve ce caractère au cours de la procédure de test, vous recevrez un message d'erreur et la vérification est interrompue. Dans ce cas, modifiez le nom du dossier ou copiez les fichiers dans un autre dossier.



Cet avertissement apparaît lorsque vous venez de modifier une liste de logiciels à l'aide de T1.prg et vous quittez VIRtuel sans enregistrer les modifications effectuées. Cliquez sur la case OK si vous ne désirez pas enregistrer les modifications. Sélectionnez la case Sauvegarder si vous désirez sauvegarder les modifications dans un fichier avec le même nom. La case Annuler vous permet d'interrompre la procédure en cours et poursuivre votre travail avec T1.prg.

❒ 4.5.3. Vérification automatique ("Petit" Diagnostic)

Une vérification automatique des variables système a lieu chaque fois que vous démarrez votre ordinateur, à condition d'avoir installé T2.acc au préalable, suivant les instructions fournies dans la section 4.4. Si vous désirez intégrer d'autres logiciels à la procédure de test automatique, placez le fichier Teste.vir dans le dossier qui contient le programme T2.acc, qui n'est autre que le dossier principal du lecteur d'initialisation.

Le test automatique concerne uniquement les logiciels intégrés à Atari Desktop ou les programmes compatibles avec l'environnement GEM, comme par exemple, WordPlus, T1.prg, Detective ou CopyStar ; Dosshell et TLDU n'en font pas partie. Si vous désirez desactiver la procédure de test automatique sur certains logiciels, il vous suffit de supprimer le fichier Teste.vir dans le répertoire

principal. Si vous désirez desactiver la vérification automatique des variables système et des logiciels, supprimez tout simplement T2.acc dans le répertoire principal.

❒ 4.5.3.1. Constituer une liste de logiciels

Le test automatique à intervalle régulier exige que la liste de logiciels, Teste.vir, et le programme T2.acc soient placés dans le même dossier. La vérification automatique s'applique uniquement aux disques durs, étant donné que l'accès aux lecteurs de disquettes provoquerait un délai d'attente trop long.

Pour être identifiée par T2.acc, la liste de logiciels doit porter le nom de Teste.vir. Vous pouvez y stocker jusqu'à 30 logiciels. Pour dresser la liste des logiciels, procédez comme suit :

Première étape

Si vous ne l'avez pas encore fait, installez VIRtuel suivant les instructions fournies dans la section 4.4.

Deuxième étape

Sélectionnez les programmes que vous voulez soumettre à un test régulièr. Choisissez en priorité les logiciels que vous utilisez le plus souvent, car ils sont plus vulnérables en cas d'infection. Ajoutez également les accessoires de bureau que vous utilisez couramment : traitement de texte, base de données, Compilateur, T1.prg et T2.acc, Foldr150.prg, etc...

Troisième étape

Placez les disquettes originales de tous les logiciels sélectionnés à portée de main, ou du moins les versions dont vous êtes sûrs qu'elles ne contiennent pas de virus.

Quatrième étape

Assurez-vous que les programmes stockés sur votre disque dur correspondent aux originaux. Si vous n'en êtes pas convaincu, recopiez l'original sur le disque dur. Ceci vous permettra d'assurer

un environnement sain pour VIRtuel et d'atteindre un degré de protection optimal.

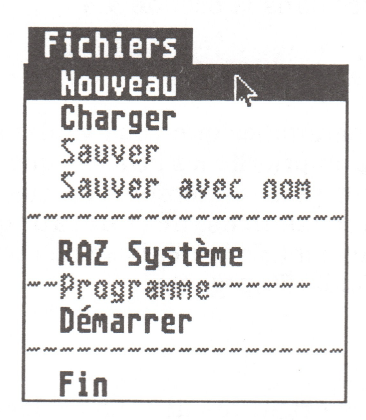
Cinquième étape

Lancez T1.prg. Si le fichier VIRtuel.dat n'a pas été chargé, (vous en serez avertis par un message), cliquez la case OK. Dans la boîte de sélection qui s'affiche maintenant sur votre écran, cliquez sur la case Annuler.

Sixième étape

Dans le menu Fichier, sélectionnez l'option "Nouveau" pour créer une nouvelle liste de logiciels. A la demande du système, localisez l'original du logiciel dans la boîte de sélection et cliquez sur la case OK pour confirmer. VIRtuel lit les valeurs initiales du programme sélectionné pour les intégrer à la liste.

Dans un second temps, sélectionnez la copie de travail correspondante sur le disque dur et cliquez sur la case OK.



Si le programme original et la copie de travail ne portent pas le même nom, vous recevrez un message. Dans ce cas, recommencez la sixième étape.

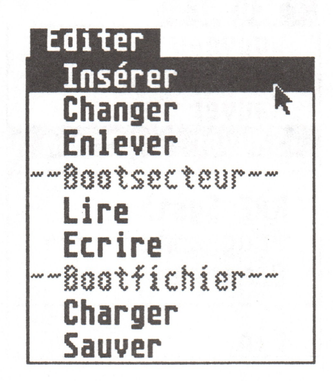
Si vous avez exécuté cette opération correctement, le nom du programme sélectionné s'inscrit en vidéo inversée dans la partie supérieure de la boîte tandis qu'en bas de la boîte apparaissent les

valeurs spécifiques du programme, qui serviront de point de départ lors d'un examen ultérieur.

Septième étape

Pour introduire un second programme dans la liste, cliquez sur l'option "Insérer" dans le menu Edition.

Comme dans l'étape précédente, sélectionnez le programme désiré et localisez, à la demande du système, la copie de travail correspondante sur le disque dur. Si le programme sélectionné figure déjà dans la liste, vous recevrez un message d'avertissement. Recommencez la septième étape.



Si vous avez exécuté cette opération correctement, vous verrez apparaître le nom du programme dans la partie supérieure de la boîte et les valeurs d'origine associées dans la partie inférieure. Tous les nouveaux programmes sélectionnés apparaissent en vidéo inversée.

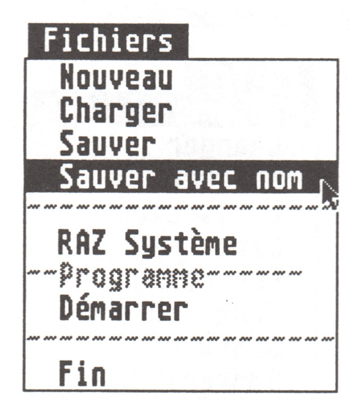
Huitième étape

Exécutez la septième étape pour chaque nouveau programme, jusqu'à ce que vous ayez réuni tous les logiciels que vous désirez soumettre à la vérification automatique.

Neuvième étape

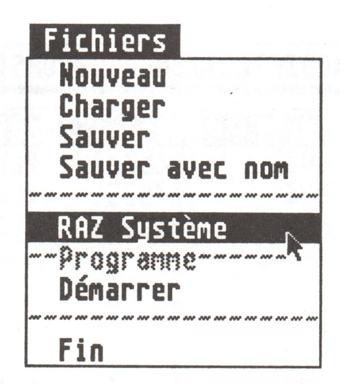
Les programmes sélectionnés se trouvent à présent dans la mémoire de travail. Pour enregistrer cette liste sur votre disque dur, sélectionnez l'option "Sauver avec nom" dans le menu Fichier.

Attribuez à votre liste de logiciels le nom Teste.vir pour permettre à T2.acc de la charger le moment voulu. Dans la boîte de sélection qui s'affiche maintenant sur votre écran, enregistrez la liste de logiciels dans le dossier qui contient T2.acc, à savoir, le répertoire principal du disque dur. T1.prg se charge de spécifier le chemin d'accès et le nom de fichier correspondant.



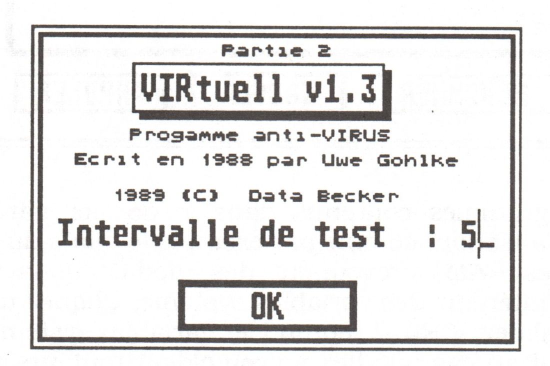
Dixième étape

Jusqu'ici nous avons établi une liste de logiciels et nous l'avons enregistrée sur le disque dur. Réinitialisez maintenant votre ordinateur de façon à intégrer les nouveaux programmes à la procédure de test automatique. Pour cela, sélectionnez l'option "RAZ Système" dans le menu Fichiers. Avez-vous bien pris soin de sauvegarder la liste de logiciels ? Si vous ne l'avez pas encore fait, recommencez la neuvième étape.



Onzième étape

Après la réinitialisation du système, l'écran affiche une boîte qui vous signale que la vérification automatique est en cours. Pour confirmer, cliquez sur la case OK.



Si au lieu de cette boîte vous recevez un message d'avertissement, consultez la section 4.5.3.4 pour vous aider à comprendre ce message. Si après la réinitialisation du système il ne se passe rien, cela peut avoir deux raisons : soit vous avez mal installé le programme VIRtuel, soit le programme T2.acc ne se trouve pas dans le bon dossier. Relisez la section 4.4 et recommencez la procédure d'installation.

Votre écran affiche une boîte qui vous signale les modifications apportées aux variables système. Cela signifie que les variables système ne correspondent plus au programme original. Pas de panique !

MODIFICATION VECTEURS

Nom :	Adr. :	est:	doit:
ETVTIM	400	fcb3e4	fcb3c6
ETVCRT	404	fdd25c	fc07c0
ETVTRM	408	fc0652	f27e
HDBPB	472	1a4e6	fc173c
HDVRW	476	a8d0	fc1a24
HDMEDI	47e	a8e6	fc18ec

RENOMMER SAUVER ANNULER

Certains programmes contenus dans le dossier par défaut du lecteur d'initialisation, comme par exemple le pilote du disque dur et les disques RAM, provoquent des modifications tout à fait normales à l'intérieur des variables système. Cliquez tout d'abord sur la case Valider. VIRtuel reprend les variables système modifiées et vous avertit au cas où elles ne coïncident toujours pas. Restez vigilant et essayez de déterminer quel est le programme qui a provoqué ces modifications.

Pour connaître la signification des autres cases, lisez la section 4.5.2.4. Si la boîte qui apparaît sur votre écran signale une modification de fichier, consultez la section 4.5.3.4. qui fournit toutes les indications nécessaires.

❐ 4.5.3.2. Modification de la liste de logiciels

Il s'avère parfois nécessaire de modifier la liste de logiciels et ceci pour différentes raisons :

❶ Vous avez décidé d'inclure de nouveaux programmes dans votre liste

❷ Vous désirez supprimer un certain nombre de programmes de la liste afin de les dispenser de la vérification automatique

❸ Vous désirez changer la version d'un programme figurant dans liste, sur le disque dur.
Si vous ne remettez pas votre liste de logiciels à jour, T2.acc vous signale une modification de programme, étant donné que les valeurs de l'original ne correspondent plus à la copie de travail stockée sur votre disque dur.

❹ Sur votre disque dur, vous avez modifié ou supprimé un programme qui figure dans la liste de logiciels soumise à la vérification automatique.

❺ VIRtuel vous signale qu'un fichier a été modifié et vous désirez mettre à jour votre liste de logiciels.

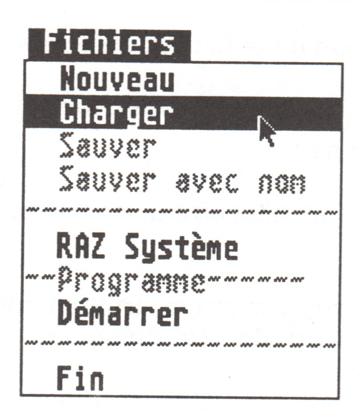
Pour modifier la liste de logiciels, procédez comme suit :

Première étape

Lancez T1.prg. Si le fichier VIRtuel.dat n'a pas été chargé, vous recevrez un message d'avertissement. Cliquez sur la case OK. Dans la boîte suivante, sélectionnez la case Annuler.

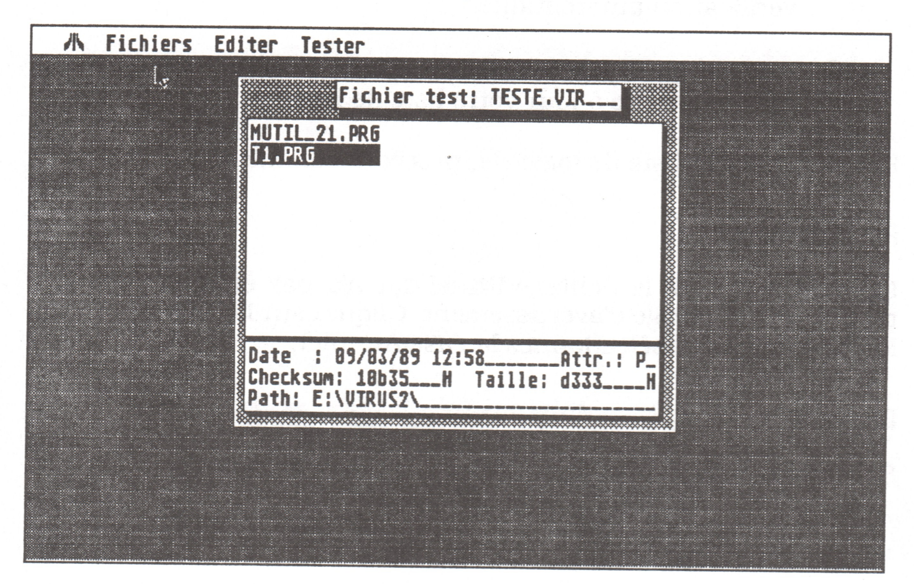
Deuxième étape

Sélectionnez l'option "Charger" dans le menu Fichier



Dans la boîte de dialogue qui s'affiche maintenant sur votre écran sélectionnez la liste de logiciels que vous désirez modifier et cliquez sur la case OK pour confirmer. La liste de logiciels s'intitule Teste.vir. La boîte affiche les noms des programmes contenus dans la liste.

Si vous tentez de charger des fichiers qui n'ont pas été créés par T1.prg et qui ne comportent pas le format standard des listes de logiciels, vous recevrez un message d'avertissement.



Troisième étape

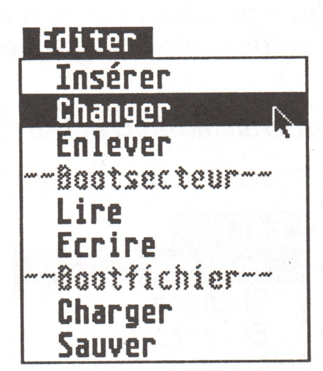
Vous pouvez maintenant apporter toutes les modifications désirées : charger ou effacer une entrée ou alors insérer un nouveau programme dans la liste.

Modifier une entrée dans la liste de logiciels

Avec la souris, pointez sur le nom du programme que vous désirez modifier et cliquez une seule fois sur le bouton gauche. Le nom du programme apparaît en vidéo inversée. Les valeurs associées au programme sélectionné s'affichent en bas de la boîte.

Pour sélectionner un programme, vous pouvez également déplacer le curseur à l'aide des touches de direction. Sélectionnez l'option "Changer" dans le menu "Editer".

Suivez la démarche employée lors de l'insertion d'un nouveau programme dans la liste que nous avons évoquée dans la septième étape sous 4.5.3.1. Pour cela, sélectionnez d'abord le programme original et localisez ensuite la copie de travail correspondante sur le disque dur.



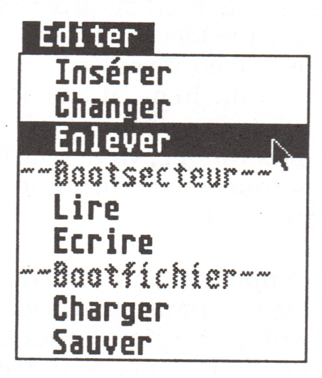
Si le programme sélectionné figure déjà dans la liste des logiciels, vous recevrez un message d'erreur. Recommencez l'opération en spécifiant un autre nom de programme et sélectionnez à nouveau l'option "Changer" dans le menu "Editer".

Le champ de sélection affiche maintenant le nom du nouveau fichier. Les valeurs associées à ce programme apparaissent en bas

de la boîte. Procédez de la même façon pour tous les programmes que vous désirez modifier.

Supprimer une entrée dans la liste de logiciels

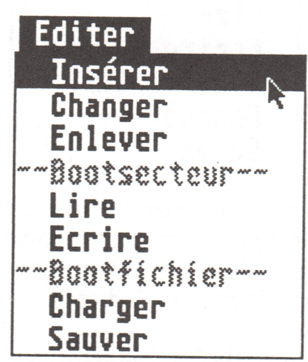
Avec la souris, pointez sur le programme que vous désirez enlever de la liste et cliquez sur le bouton gauche. Le nom du programme apparaît en vidéo inversée. Sélectionnez maintenant l'option "Enlever" dans le menu "Editer".



Le nom du programme disparaît de la liste et tous les programmes suivants avancent d'une position pour combler l'espace vide. Pour supprimer plusieurs entrées, répétez cette opération aussi souvent que nécessaire.

Insérer un nouveau programme dans la liste

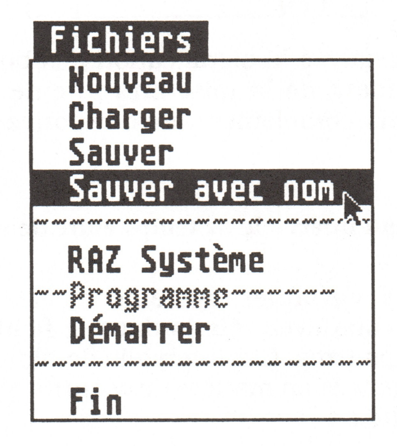
Sélectionnez l'option "Insérer" dans le menu "Editer".



Comme dans les opérations précédentes, le système vous invite à sélectionner le programme original et à localiser la copie de travail sur le disque dur. Si le programme sélectionné figure déjà dans la liste, un message d'avertissement s'affiche sur l'écran et vous devrez recommencer l'opération. Si tout s'est déroulé normalement, le nom du nouveau programme s'affiche dans la partie supérieure tandis que les valeurs d'origine associées apparaissent en bas de la boîte.

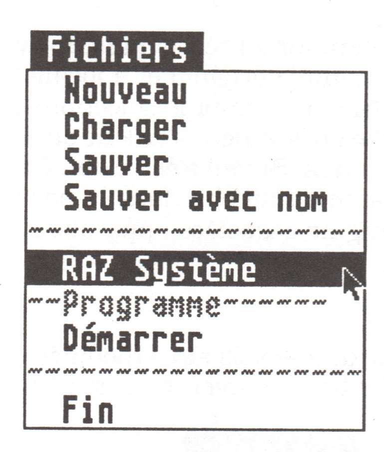
Quatrième étape

Sauvegardez la liste de logiciels ainsi modifiée sous le nom Teste.vir en sélectionnant l'option "Sauver avec nom" du menu Fichier.



Cinquième étape

Réinitialisez votre système pour que les modifications apportées à la liste de logiciels soient prises en compte par T2.acc lors de la prochaine vérification. Pour cela, sélectionnez l'option "RAZ Système" dans le menu Fichier.



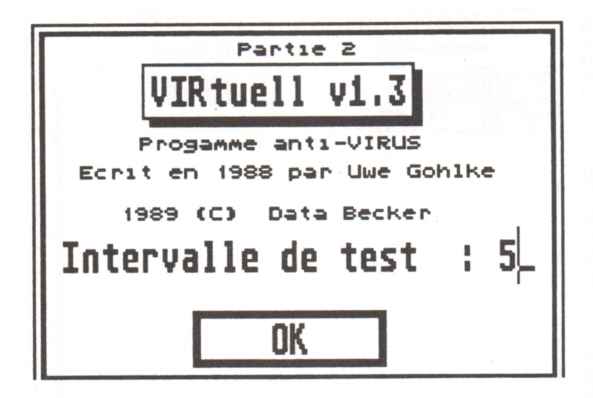
Nous avons déjà analysé la signification des boîtes de T2.acc qui s'affichent au moment de la mise en route de l'ordinateur. Pour toutes informations complémentaires, reportez-vous à la section 4.5.3.1.

❒ 4.5.3.3. Définir un intervalle de temps entre deux vérifications

T2.acc vérifie les variables système et, le cas échéant, les programmes que vous avez réunis dans le fichier Teste.vir à des intervalles de temps fixes. Cet intervalle de temps doit refléter vos besoins et vos exigences en matière de sécurité. Pour cela, procédez de la façon suivante :

Première étape

Sélectionnez l'option "VIRtuel Info" dans le menu Atari à partir d'un programme permettant d'accéder aux accessoires, comme par exemple Atari Desktop. Le système affiche une boîte avec la mention de copyright et l'intervalle de temps défini entre deux vérifications.



Deuxième étape

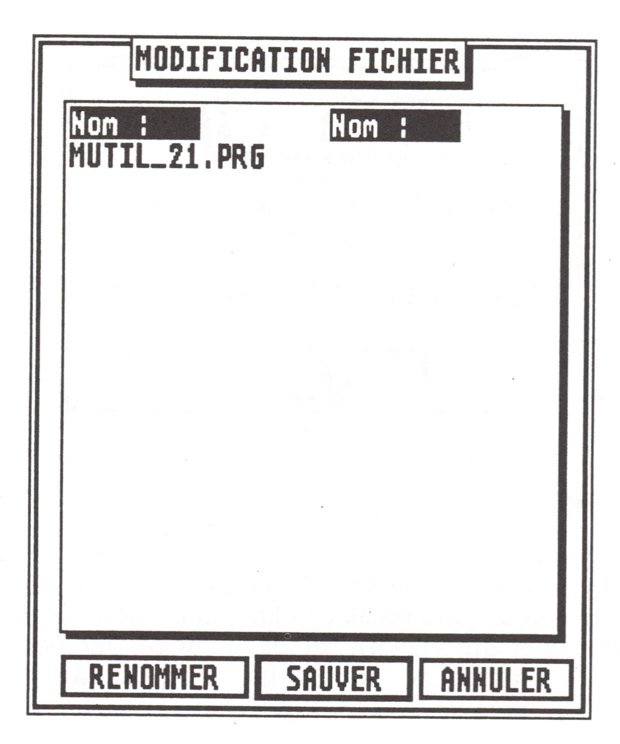
Le champ destiné à l'intervalle de temps comporte la valeur par défaut 5. Cela signifie qu'une vérification automatique aura lieu toutes les minutes. Vous pouvez définir une valeur comprise entre 1 et 20 minutes qui restera valide jusqu'au moment ou vous déciderez vous-même de la modifier ou jusqu'au moment de réinitialiser le système.

❒ 4.5.3.4. Messages d'avertissement

Si T2.acc a été installé correctement, suivant les instructions fournies dans la section 4.4 et si vous avez déjà constitué un fichier Teste.vir, le système procède à une vérification régulière des programmes spécifiés. T2.acc vous signale toutes les modifications survenues à l'intérieur des programmes par une série de messages qui apparaissent dans une boîte de dialogue. VIRtuel est capable de reconnaître les modifications suivantes :

- Suppression de la copie de travail

- Modification des valeurs associées à la copie de travail : checksum, taille du fichier, date de création, caractéristiques ou nom du fichier.



Cette boîte affiche les noms des programmes modifiés. Les modifications ont été détectées à la suite d'une comparaison entre les copies de travail stockées sur le disque dur et les valeurs spécifiées dans le fichier Teste.vir. Cette boîte vous offre trois possibilités de sélection :

Renommer

Cette option permet de valider les valeurs associées aux copies de travail qui serviront désormais de référence pour toutes les vérifications qui vont suivre.

Sauver

Cette option permet d'écrire la liste des noms modifiés dans un fichier de texte de contrôle.

Annuler

Cette option permet d'ignorer le message d'avertissement.

Réfléchissez un instant avant de choisir l'une de ces trois options. Les modifications de fichiers peuvent avoir plusieurs origines qui exigent un traitement différent :

- Peut-être avez-vous modifié le programme vous-même
- Certains programmes modifient leur code directement sur le support de stockage.
- Le programme a été infecté par un virus

Si vous avez vous-même opéré des modifications sur un programme (peut-être l'avez-vous protégé en écriture ou effectué un changement de version), vous pouvez tranquillement sélectionner la case Valider. Les valeurs modifiées sont à présent validées et vous recevrez un nouveau message d'avertissement lorsqu'elles subiront une nouvelle modification.

Au moment de la réinitialisation, le système vous signale les mêmes modifications pour la simple raison que ces nouvelles valeurs ne figurent pas encore dans la liste de logiciels enregistrée dans le fichier Teste.vir.

Si vous désirez rendre ces valeurs permanentes, réactualisez la liste des logiciels selon la méthode que nous avons évoquée dans la section 4.5.3.2.

Si vous n'avez pas modifié le programme vous-même, sélectionnez l'option Sauver pour sauvegarder la liste des logiciels modifiés et consultez le fichier T2daerr.cmp généré par T1.prg, qui réunit tous les programmes modifiés.

Cette opération vous permet de prendre connaissance des modifications enregistrées ou de détecter un Link-virus. La modification du checksum et de la taille du fichier est un symptôme caractéristique des Link-virus.

Pour plus de précisions sur l'interprétation de ces fichiers de texte, consultez la section 4.7. Pour toutes informations complémentaires, reportez-vous aux sections 4.1 et 4.3.

Ne relancez jamais un programme modifié car, s'il a été contaminé, le virus pourrait se propager.

Modification de vecteurs

Si T2.acc a été installé correctement, suivant les instructions fournies dans la section 4.4, le programme effectue un examen régulier des principales variables système. T2.acc vous signale toutes les modifications par une série de messages qui apparaissent dans une boîte de dialogue.

Cette boîte de dialogue affiche les variables modifiées avec leurs adresses, leur contenu à un moment donné et leur valeur initiale et vous offre trois possibilités de choix :

Renommer

Les variables système modifiées sont validées et serviront désormais de référence pour toutes les vérifications qui vont suivre.

MODIFICATION VECTEURS

Nom :	Adr.:	est:	doit:
ETVTIM	400	fcb3e4	fcb3c6
ETVCRT	404	fdd25c	fc07c0
ETVTRM	408	fc0652	f27e
HDBPB	472	1a4e6	fc173c
HDVRW	476	a8d0	fc1a24
HDMEDI	47e	a8e6	fc18ec

RENOMMER | SAUVER | ANNULER

Sauver

La liste des variables système modifiées est enregistrée dans un fichier de texte.

Annuler

Aucune action.

Voici quelques indications qui vous aideront à mieux comprendre la finalité d'une vérification des variables et l'importance des modifications enregistrées :

Le système d'exploitation d'Atari utilise des variables en guise de pointeurs sur un certain nombre de fonctions déclenchées soit par un état particulier de l'ordinateur, par une action délibérée de l'utilisateur. Par exemple, si vous effectuez une copie d'écran en utilisant la séquence de touches ALT+HELP, le système d'exploitation exécute la fonction indiquée par le contenu de HRDCPY. Cette fonction se charge en principe d'effectuer une copie d'écran.

Cette variable peut être modifiée afin de pointer sur une autre fonction, chargé par exemple d'effectuer une copie d'écran améliorée. Dans le cas présent, le programme manipule les variables dans un but constructif. Mais en même temps, ce mécanisme permet de mettre en oeuvre un certain nombre de fonctions beaucoup moins utiles et parfois même destructrices, comme par exemple, effacer des programmes et des fichiers importants.

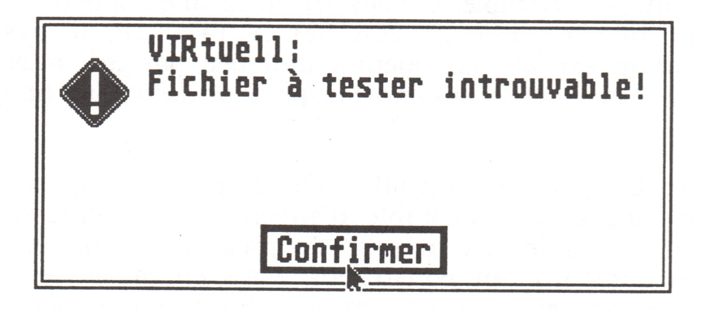
Quoi qu'il en soit, T2.acc détecte toutes ces modifications et vous les signale à l'intérieur d'une boîte de dialogue. A vous de déterminer si la modification des variables est due à une manipulation interne inoffensive ou si elle a été provoquée par un virus.

Certains programmes modifient les variables système de façon légale : les pilotes de disques durs, les utilitaires chargés d'effectuer des copies d'écran, les disques RAM,l'horloge du système et autres programmes activés à partir du lecteur par défaut au moment de la mise en route de l'ordinateur. Lorsque vous installez ce type de programmes, le système vous signale en principe un certain nombre

de modifications dans les variables système après la réinitialisation de l'ordinateur.

D'autre part, les variables système peuvent être modifiées pendant l'activité du système, à chaque lancement des programmes que nous avons mentionnés plus haut. Avec l'expérience, vous serez en mesure de repérer les programmes qui provoquent des modifications à l'intérieur des variables système. Cependant, méfiez-vous lorsqu'un programme modifie soudainement celles-ci alors qu'il ne l'avait jamais fait auparavant. Cette modification pourrait être le résultat d'une manipulation malveillante du programme. Vous trouverez dans l'annexe de ce livre une liste de logiciels avec les variables qu'ils modifient.

Pour connaître la démarche à adopter en cas de modification des variables système, consultez les sections 4.1 et 4.3.



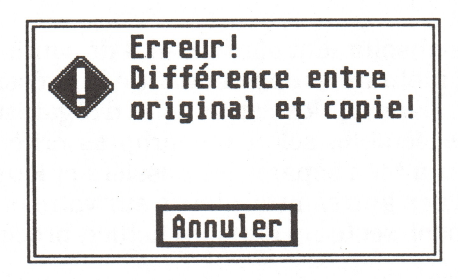
Ce message indique que le fichier Teste.vir est introuvable. Cet avertissement s'affiche lorsque T2.acc ne parvient pas à trouver le fichier Teste.vir dans le dossier d'initialisation au moment de la mise en route de l'ordinateur. La vérification automatique ne peut donc pas avoir lieu.



Ce message apparaît lorsque T2.acc n'a pas trouvé le fichier Teste.vir qui contient la liste des logiciels à examiner.



Ce message d'avertissement s'affiche lorsque vous spécifiez un nom de fichier et un chemin d'accès qui existent déjà dans la liste de logiciels. Les noms des programmes contenus dans cette liste doivent être uniques.



Ce message d'avertissement apparaît lorsque le nom du programme original que vous avez spécifié ne coïncide pas avec le nom de la copie de travail correspondante.

❐ 4.5.4. Archiver les boot-secteurs

Lorsque le système est mis en route, T1.prg examine le fichier VIRtuel.dat, qui contient des informations sur les boot-secteurs exécutables reconnus inoffensifs. Parallèlement, vous pouvez enregistrer d'autres boot-secteurs dans une série de fichiers et les placer dans un dossier spécifique. La disquette originale contient un dossier appelé Boots, que vous pourrez utiliser pour cela.

Ces fichiers vous permettront de récupérer les boot-secteurs au cas où ils seraient endommagés par une action malveillante ou une erreur quelconque. Cependant, vous devez sauvegarder les fichiers contenant des boot-secteurs en fonction de leur emploi ultérieur.

❶ Lorsque vous sauvegardez ces fichiers uniquement pour constituer des archives, utilisez une disquette spécialement prévue pour cela. Ne sauvegardez pas sur cette disquette les boot-secteurs infectés ou ceux que vous soupçonnez d'être contaminés par un virus.

❷ Placez les boot-secteurs que vous avez stockés dans le dossier Boots parallèlement au fichier VIRtuel.dat, dans un autre dossier spécialement prévu pour cela.

Le mieux serait de mettre dans le dossier Boots les boot-secteurs utilisés pour une application particulière, comme par exemple les jeux, et qui ne figurent pas encore dans le fichier VIRtuel.dat.

Si vous n'êtes pas absolument sûrs de l'état de santé de vos secteurs et si vous avez le moindre soupçon quant à la présence d'un virus, ne les copiez pas dans ce dossier. A vous d'organiser votre travail comme bon vous semble, selon vos propres critères et besoins. Cependant, veillez à bien séparer les dossiers et leur contenu pour faciliter le travail des autres utilisateurs sur votre ordinateur. Pour sauvegarder les boot-secteurs dans un fichier, procédez de la façon suivante :

Première étape

Lancez T1.prg. Si le fichier VIRtuel.dat n'a pas été chargé, vous recevrez le message d'avertissement correspondant. Cliquez sur la case Annuler pour quitter le programme et copiez le fichier VIRtuel.dat dans le dossier qui contient T1.prg. Relancez T1.prg. Pour toutes informations complémentaires sur ce message d'avertissement, consultez la section 4.5.3.4.

Choisir répertoire boot

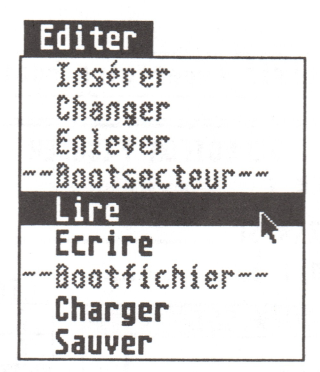
SELECTEUR FICHIER
Répertoire :
E:\VIRUS2*.SCT
Sélection :
LECTEUR
*.SCT
BOOTS
MODIF
ST
STE
A B C D E F G H I J K L M N O P
OK
Annuler

Si vous avez déjà stocké des boot-secteurs dans un dossier et si vous voulez les soumettre à une vérification, localisez le dossier correspondant dans la boîte de sélection qui s'affiche sur votre écran et cliquez sur la case OK pour confirmer.

Rappelez-vous que T1.prg considère les boot-secteurs stockés dans ce fichier comme inoffensifs. Prenez donc soin de sauvegarder dans ce dossier uniquement les fichiers qui réunissent ces conditions. Si vous n'avez pas encore créé un fichier de boot-secteurs, cliquez sur la case Annuler.

Deuxième étape

Sélectionnez l'option "Lire" dans la partie Bootsecteur du menu "Editer".



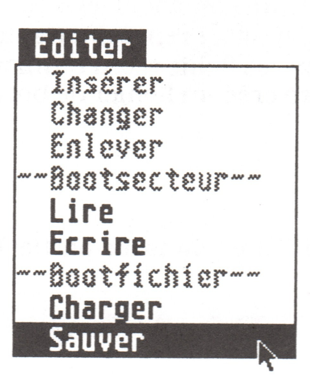
Placez ensuite la disquette qui contient le boot-secteur à archiver dans le lecteur A: ou B: et sélectionnez le lecteur utilisé dans la boîte de dialogue.

Cliquez sur la case OK pour confirmer votre choix. La boîte suivante affiche toutes les informations relatives au boot-secteur que vous venez de charger dans la mémoire de travail.

Pour tous détails supplémentaires sur ces informations, lisez le paragraphe 4.5.2.1. Veillez à ne pas copier des boot-secteurs inconnus ou infectés par des virus.

Troisième étape

Sélectionnez maintenant l'option Sauver du menu "Editer" pour enregistrer le boot-secteur que vous venez de charger, dans un fichier.

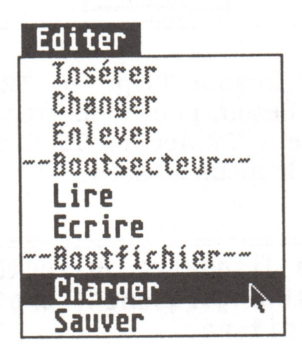


☛ **Attention :** Veillez à ne pas confondre l'option "Ecrire" de la rubrique Bootsecteur qui permet de copier le contenu du secteur chargé dans la mémoire sur un autre secteur, avec l'option "Sauver" de la rubrique Bootfichier utilisée pour générer un nom de fichier.

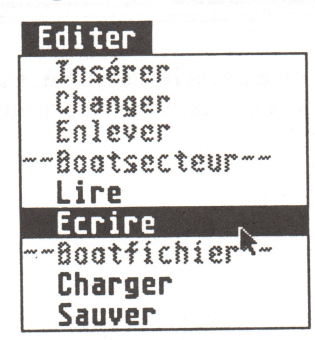
Dans la boîte qui s'affiche sur votre écran, sélectionnez un nom de fichier qui est dans la disquette, avec l'extension standard .sct et cliquez sur la case OK pour confirmer. Gardez à portée de main une disquette réservée à l'archivage des boot-secteurs.

Quatrième étape

Pour récupérer le contenu des boot-secteurs archivés, sélectionnez l'option "Charger" du menu "Editer".

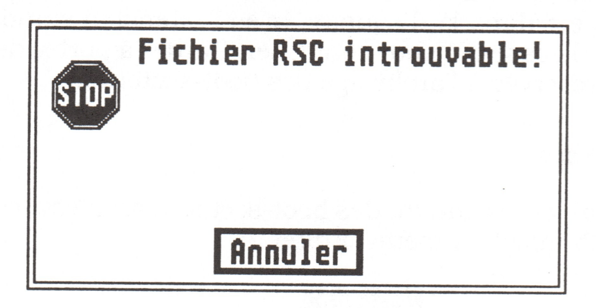


Dans la boîte qui s'affiche sur votre écran, sélectionnez un fichier avec l'extension standard .sct. et exécutez la commande "Ecrire" du menu "Editer" pour enregistrer le boot-secteur sur une disquette.

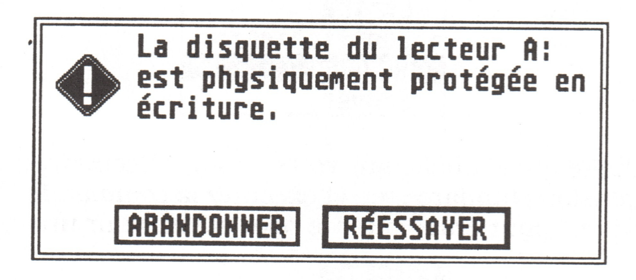


Pour toutes informations complémentaires, lisez les paragraphes 5.1 et 5.3.

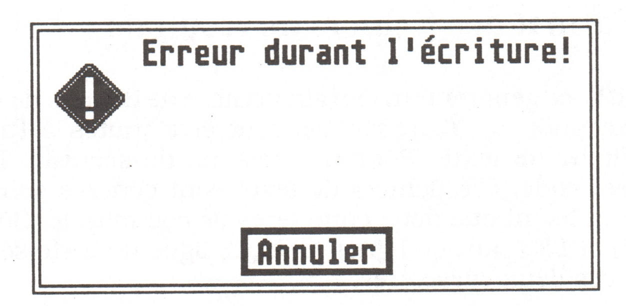
❐ 4.6. Messages d'erreurs



Ce message apparaît lorsque T1.prg ou T2.acc n'a pas trouvé le fichier .rsc dont il a besoin pour démarrer. Les fichiers T1.prg et T1.rsc et les fichiers T2.acc et T2.rsc doivent se trouver respectivement dans le même dossier.

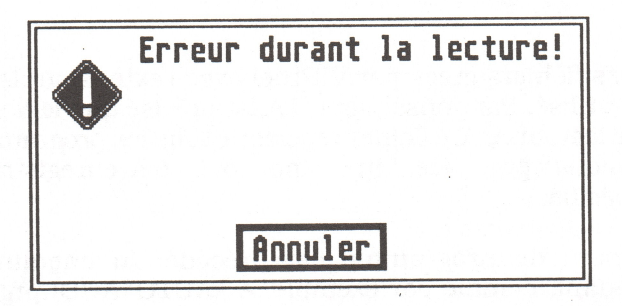


La disquette qui se trouve dans le lecteur A: est protégée en écriture. Supprimez la protection et essayez encore une fois !



Ce message d'erreur peut avoir différentes origines :

- La disquette est pleine
- La disquette est protégée en écriture
- Lecteur inexistant
- Erreur d'ordre matériel sur le support de stockage



Comme pour le message précédent, cette erreur peut avoir différentes origines :

- Lecteur inexistant
- Fichier absent
- Format de fichier incorrect
- Erreur d'ordre matériel sur le support de stockage

❒ 4.7. Format des fichiers de résultats

T1.prg et T2.acc génèrent un certain nombre de fichiers de résultats qui, à l'exception de Teste.vir, peuvent être traités à l'aide d'un simple éditeur de texte. Pour des raisons de sécurité, le fichier Teste.vir est codé. Les fichiers de texte sont générés sous format ASCII et n'utilisent que deux caractères de commande, CR (Retour de chariot) et LF (Saut de ligne). Chaque ligne de texte se termine par un de ces deux caractères.

Les noms des fichiers que nous allons décrire dans les pages qui suivent ont été sélectionnés dans les boîtes proposées par VIRtuel. Pour vous simplifier la tâche, reprenez ces noms tels quels.

La lettre x contenue dans le nom du fichier représente le lecteur (A, B, C...). Ce format facilite l'association entre les fichiers de résultats créés par T1.prg ou T2.acc et le lecteur.

Lx.lst

Le nom des fichiers créés par VIRtuel avec l'extension .lst indique le lecteur utilisé. Par conséquent, LA.lst précise que le fichier a été créé sur le lecteur A:. Ce fichier répertorie tous les programmes avec les extensions .prg, .acc, .ttp, .app, .ovl, .tos enregistrés sur le lecteur spécifié.

Chaque nom de programme est précédé du chemin d'accès correspondant, comme par exemple, A:\AUTO\AHDI.prg. Le nom du programme est suivi de l'attribut du fichier, la date et l'heure de sa création, la taille du fichier et le checksum. Si T1.prg détecte, lors d'un diagnostic, un programme infecté par un Link-virus, le nom du virus apparaît derrière le checksum.

Lx.bak

Les fichiers générés par VIRtuel avec l'extension .bak présentent l'état précédent des programmes enregistrés sur le lecteur spécifié et serviront de référence lors d'une prochaine comparaison. Lx.bak présente la même structure que les fichiers .lst. Ce n'est que l'extension qui est différente.

Lx.lvs

Les fichiers générés par VIRtuel avec l'extension .lvs présentent une liste des logiciels infectés par un virus connu sur le lecteur spécifié. LA.lvs contient par conséquent la liste des logiciels infectés sur le lecteur A:.

Ce fichier répertorie tous les programmes infectés avec les extensions .prg, .acc, .ttp, .app, .ovl, .tos, enregistrés sur le lecteur spécifié. Le nom du programme est suivi de son attribut, la date et l'heure de sa création, la taille du fichier, le checksum et le type du virus détecté.

Lx.cmp

Les fichiers générés par VIRtuel avec l'extension .cmp présentent la liste des programmes modifiés, enregistrés sur le lecteur spécifié. LA.cmp contient par conséquent la liste des programmes modifiés sur le lecteur A:. Ce fichier répertorie tous les programmes modifiés avec les extensions .prg, .acc, .ttp, .app, .ovl, .tos sur le lecteur correspondant. Les informations sont organisés de la façon suivante :

- Chemin d'accès et nom du programme
- Les valeurs initiales décrivant l'état du programme avant sa modification, c'est-à-dire, les valeurs enregistrées lors du dernier diagnostic.

La liste des logiciels modifiés est suivie d'une autre liste qui répertorie les derniers programmes sélectionnés.

T2DAERR.cmp

Le fichier T2DAERR.cmp est généré par T2.acc après une vérification automatique qui a révélé des modifications dans un programme répertorié dans Teste.vir. Mais pour cela, vous devez cliquer sur la case Enregistrer dans la boîte de dialogue. Ce fichier contient une liste de logiciels modifiés qui présente la structure suivante :

- Chemin d'accès et nom du programme modifié
- Valeurs du programme original

- Valeurs modifiées de la copie de travail

Pour améliorer la lisibilité, la signification de chaque valeur est présentée sous forme d'en-tête.

T2 VIERR.cmp

Le fichier T2VIERR.cmp est généré par T2.acc au cours de la vérification automatique ayant révélé des modifications dans les variables système. Mais pour cela, vous devez cliquer sur la case Sauver dans la boîte de dialogue. Ce fichier contient la liste des variables système modifiées et se compose comme suit :

- Nom des variables système
- Adresses des variables système dans la mémoire
- Nouveau contenu des variables système
- Valeur initiale des variables système

Par souci de lisibilité, la signification des valeurs est présentée sous forme d'en-tête.

Teste.vir

Le fichier Teste.vir est constitué à l'aide de T1.prg et répertorie les programmes soumis à une vérification régulière, que nous avons réunis dans la liste des logiciels. Pour des raisons de sécurité, ce fichier est codé et ne peut pas être lu par un programme de traitement de texte.

Bootsct.sct

Le fichier Bootsct.sct est créé par T1.prg et présente le contenu du boot-secteur d'une disquette. Ce fichier peut être traité à l'aide d'un contrôleur de disquettes.

VIRtuel.dat

Le fichier VIRtuel.dat est livré sur la disquette originale et contient une liste de boot-secteurs connus et inoffensifs. Ce fichier ne doit pas être modifié, sinon, T1.prg ne pourra plus le lire.

Chapitre 5

Que faire en cas d'infection ?

❐ 5.1. Critères d'infection

Ce n'est qu'après avoir prouvé l'existence d'un code viral dans la mémoire de l'ordinateur ou sur un support de stockage associé, que l'on peut affirmer avec certitude qu'un système est infecté. En plus de cela, la présence d'un virus ne peut être prouvée qu'en connaissance du code viral, d'où la difficulté de détecter les virus inconnus.

Pour ce qui est des virus connus, le programme VIRtuel peut facilement prouver leur présence en effectuant une comparaison entre le code viral et le code des programmes, si bien qu'une intervention rapide peut encore éviter la catastrophe. Lorsque VIRtuel identifie un virus, il affiche un message précisant sa nature : virus d'initialisation ou link-virus. Mais à ce moment, votre système, ou du moins la disquette examinée, a déjà succombé au virus.

Si cela arrive, consultez les paragraphes 5.3.1 et 5.3.2 qui vous expliquent comment procéder pour décontaminer votre système. Si VIRtuel vous signale des modifications inhabituelles à l'intérieur de votre logiciel, lisez les indications suivantes pour déterminer avec certitude si votre système est infecté.

Lorsque VIRtuel identifie un boot-secteur exécutable sans toutefois signaler la présence d'un virus, vous avez la possibilité d'examiner

vous-même les instructions contenues dans le boot-secteur. Ceci exige toutefois une certaine expérience dans la programmation en assembleur.

Le premier indice sur l'origine du boot-secteur vous est fourni par les programmes stockés sur la disquette. La disquette peut contenir des jeux ou autres programmes qui sont lancés à partir d'un boot-secteur exécutable.

Si vous ne connaissez pas la nature des instructions contenues dans le boot-secteur, vous devez archiver ce secteur suivant les indications fournies dans la section 5.4 et immuniser la disquette.

Effectuez tout d'abord un test pour déterminer si le boot-secteur effacé par l'opération d'immunisation était effectivement utilisé par l'un des programmes stockés sur la disquette - certains programmes ne fonctionneront plus. Si tel est le cas, votre boot-secteur est inoffensif et vous pouvez le retransférer sur votre disquette. Pour plus de détails sur cette opération, lisez la section 5.3.1.

Le dépistage des link-virus inconnus est relativement difficile et en particulier lorsque le virus n'a pas encore provoqué des dégats. La seule chose à faire dans un tel cas est de surveiller votre système de très près. T1.prg et T2.acc se chargent de surveiller en permanence les programmes et les variables système, dont la moindre modification peut fournir un indice précieux sur la présence éventuelle d'un virus. Cependant, les manipulations effecutées par un virus fournissent d'autres indices qu'il ne faudra pas négliger.

Par conséquent, l'utilisateur devra être particulièrement vigilant lorsque l'ordinateur se comporte de façon étrange ou lorsqu'il refuse d'exécuter certaines opérations qui ne lui posaient aucun problème auparavant. Certaines fonctions sont exécutées plus lentenment que d'habitude, le système se bloque de plus en plus souvent, la souris ne réagit plus avec la même rapidité, le clavier communique mal avec le système, etc...

En revanche, si certaines fonctions s'exécutent plus rapidement qu'auparavant (si par exemple la copie des disquettes ne dure plus que 10 secondes), l'utilisateur ne devrait pas tomber en admiration

devant les extraordinaires capacités de son ordinateur, mais plutôt vérifier si tous les fichiers ont été copiés correctement.

Si l'on songe à tout ce qui peut arriver à un ordinateur et tout ce que l'on peut effectivement mettre en pratique, notre imagination ne connaît pas de limites. Bien ou mal, peut importe. Tous les moyens sont bons. Si vous ne comprenez pas les messages d'avertissement envoyés par VIRtuel sur les modifications intervenues dans certains logiciels, consultez la section 5.3 qui explique ce qu'il faut faire dans ce cas. Votre ordinateur est très probablement infecté lorsque :

- La taille des programmes a été modifiée sans aucune intervention de votre part,
- Le checksum des programmes a été modifié,
- Certains programmes ou fichiers ont subitement disparu.

❐ 5.2. Mieux vaut prévenir que guérir

❐ 5.2.1. Où sont les dangers ?

Toute nouvelle disquette peut porter un virus. Les disquettes qui relèvent du domaine public sont particulièrement menacées, étant donné que le programmeur jouit d'un certain degré d'anonymat. Même les disquettes originales distribuées sur le marché des logiciels ne sont à l'abri d'une infection.

Pour cette raison, il convient d'être très vigilant avec toutes les disquettes, quelle que soit leur origine. Les ordinateurs qui communiquent entre eux par l'intermédiaire d'un réseau offrent un terrain idéal pour la propagation des virus et plus particulièrement lorsque le réseau est accessible à des institutions publiques et en particulier aux écoles et aux universités. Dans ce cas également, le programmeur de virus peut facilement garder l'anonymat et les chances d'identifier le coupable sont pratiquement nulles. La seule méthode de protection réellement fiable est de ne jamais allumer son ordinateur.

❒ 5.2.2.1. Dix règles d'or

Pour vous protéger le mieux possible contre une infection virale et éviter la destruction de vos données, il convient de respecter un certain nombre de règles qui vous permettront d'empêcher ou tout au moins d'enrayer la progression des virus.

1. Protégez, dans la mesure du possible, toutes vos disquettes contre l'écriture (sur les disquettes 3,5 pouces, tirez la languette dans l'encoche de protection de façon à libérer l'orifice). Ne supprimez cette protection qu'en cas de nécessité.

2. Protégez tous les logiciels et fichiers importants contre l'écriture à l'aide de commandes logicielles. Le menu fichier de Desktop vous permet de limiter l'accès aux fichiers à un simple droit de lecture.

3. Effectuez systématiquement un test de dépistage à l'aide de VIRtuel pour détecter tous les boot-virus et link-virus.

4. Installez VIRtuel T2.acc de façon à mettre en place un contrôle systématique.

5. A l'aide de VIRtuel, établissez un diagnostic sur toutes les disquettes et stockez les fichiers de résultats sur la disquette examinée. Ceci vous permettra de détecter toutes les nouvelles modifications lors du prochain diagnostic.

   Prenez les mêmes précautions avec les disquettes que vous prêtez à d'autres personnes. Ainsi, chaque utilisateur de VIRtuel pourra diagnostiquer les disquettes qui changent de main pour déterminer si elles correspondent toujours à la version enregistrée dans le fichier de diagnostic.

6. Effectuez au moins une copie de sauvegarde ou de travail de toutes les disquettes originales. Utilisez toujours votre disquette de travail et ne lancez jamais vos programmes à partir de l'original. Certains logiciels protégés contre le piratage ne vous permettent pas de faire des copies de sauvegarde. Dans ce cas, demandez à votre distributeur une copie que vous pourrez utiliser comme base de travail.

Si celle-ci est endommagée, vous pourrez avoir recours à la disquette originale.

7. Copiez sur votre disque dur uniquement les logiciels que vous utilisez régulièrement pour avoir une vue d'ensemble sur vos programmes et données et accélérer le processus de vérification.

8. N'utilisez votre disque dur qu'en cas de besoin.

9. Faites une liste avec l'origine de tous vos logiciels. De cette façon vous pourrez remonter plus facilement à la source des virus et démasquer avec un peu de chance son auteur.

10. Effectuez régulièrement des copies de sauvegarde de vos fichiers importants ; si vos données sont détruites, vous n'aurez pas tout perdu.

❒ 5.3. Décontamination

Ce chapitre explique comment détruire les boot-virus et les link-virus. Envoyez-nous toutes vos disquettes et vos programmes suspects. Nous les transmetterons à l'auteur de ce livre qui les examinera de plus près et vous communiquera ses conclusions. De cette façon, le concepteur de VIRtuel pourra adapter son programme à tous les virus encore inconnus et vous assurer un degré de protection optimal.

❒ 5.3.1.Boot-virus

Pour détruire ce type de virus, vous devez modifier le boot-secteur de votre disquette. Cette opération peut être réalisée de différentes façons. La méthode la plus simple vous est offerte par le menu Vérification de T1.prg. La boîte de dialogue qui s'affiche sur votre écran contient une commande, Immuniser, qui déclenche l'opération de remplacement de votre secteur infecté par un boot-secteur exécutable et inoffensif, protégé contre tous les virus connus.

Si vous avez initialisé votre ordinateur avec une disquette infectée à partir du lecteur A:, éteignez-le après avoir décontaminé la disquette et attendez au moins 15 secondes avant de le remettre en route. Une simple pression sur la touche Reset ne suffit pas, car certains virus resistent à cette opération et restent dans la mémoire.

T1.prg vous offre encore une autre possibilité de détruire un virus ou tout autre boot-secteur suspect : si au cours de votre travail vous avez pris soin d'archiver les boot-secteurs, vous pouvez les retransférer maintenant sur leur disquette d'origine. Ceci vous permet également de récupérer les boot-secteurs que vous avez effacés par inadvertance.

Pour plus de détails sur l'archivage des boot-secteurs, reportez-vous à la section 5.5.4. Procédez de la façon suivante :

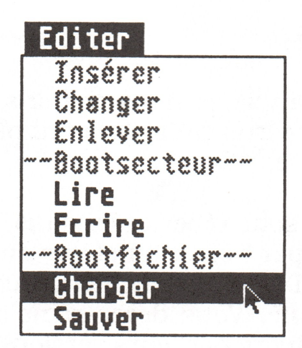
Première étape

Lancez VIRtuel T1.prg. Si le fichier VIRtuel.dat n'a pas été chargé, vous recevrez un message d'avertissement sur votre écran. Si vous avez déjà stocké vos boot-secteurs dans un dossier et si vous voulez les soumettre à une vérification, localisez le dossier correspondant dans la fenêtre de sélection qui s'affiche sur votre écran et cliquez sur la case OK pour confirmer.

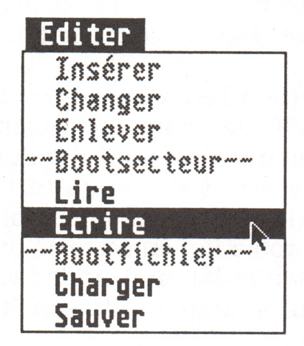
Veillez à sauvegarder dans ce dossier uniquement les fichiers exécutables qui ne présentent aucun danger, étant donné que VIRtuel T1.prg considère les boot-secteurs stockés dans ce fichier comme inoffensifs. Si vous n'avez pas encore stocké les boot-secteurs dans un fichier, cliquez sur la case Annuler.

Deuxième étape

Sélectionnez l'option "Charger" du menu Editer.



Sélectionnez le fichier qui renferme le boot-secteur désiré sur la disquette des archives et cliquez sur la case OK pour confirmer.



Troisième étape

Sélectionnez l'option "Ecrire" du menu Editer.

Placez ensuite la disquette destinée à recevoir le nouveau boot-secteur dans A: ou B:, spécifiez le lecteur dans la fenêtre qui s'affiche sur votre écran et cliquez sur la case OK pour confirmer. La troisième méthode utilisée pour modifier un boot-secteur fait appel à un contrôleur de disques. Cette méthode consiste à modifier un ou plusieurs octets sur la piste 0, secteur 1 de la disquette, à l'aide du contrôleur de disques. Prenez soin de modifier, si nécessaire, les caractéristiques d'exécution ou même détruire le boot-secteur.

❐ 5.3.2. Link-virus

La méthode la plus simple, et dans certains cas la seule possible, pour détruire un link-virus consiste à remplacer le logiciel infecté par sa version originale.

Les logiciels infectés sont répertoriés dans le fichier de résultats T2daerr.cmp, généré par T2.acc ainsi que dans les fichiers Lx.cmp et Lx.lvs générés par T1.prg. Ces fichiers précisent en outre le nom du link-virus incriminé. Vous devez remplacer tous les logiciels marqués dans ces fichiers par leurs versions originales.

Si VIRtuel détecte, lors d'un diagnostic, une série de modifications que vous n'avez pas provoquées vous-même, remplacez les programmes suspects par leur version originale après les avoir copiés sur la disquette réservée aux porteurs de virus.

Envoyez cette disquette à l'éditeur qui se chargera de la remettre au concepteur de VIRtuel pour un examen approfondi. Vous contribuerez ainsi à la mise au point d'un anti-virus efficace armé contre tous les nouveaux virus sur Atari. Si vous pensez être vous-même à l'origine de ces modifications, si vous avez, par exemple, défini une protection en écriture ou effacé le programme, ce qui exclut toute manipulation d'origine virale, vous n'aurez pas besoin de rétablir le programme dans son état d'origine.

Si le programme que vous avez vous-même modifié figure dans la liste Verif.vir, vous pouvez valider les nouvelles valeurs suivant les instructions fournies dans le paragraphe 5.3.2.

Après une contamination massive, nous vous conseillons de reformater le disque dur et les disquettes qui contiennent vos copies de travail. Cette solution peut se révéler parfois plus fiable et plus rapide que la procédure de décontamination programme par programme.

❐ 5.4. Outils de diagnostic

Ce chapitre vous présente un certain nombre de logiciels permettant d'effectuer un examen approfondi des boot-secteurs et des logiciels.

❐ 5.4.1. Le contrôleur de disquette

Le contrôleur de disquette présente des avantages considérables si vous désirez soumettre vos disquettes à un examen minutieux ou si vous décidez de modifier certains octets. Il permet d'éditer les données contenues dans le boot-secteur pour déterminer s'il contient un virus inconnu à l'heure actuelle. Cependant, la manipulation d'un contrôleur de disquettes exige une connaissance approfondie de la structure des disquettes et de la programmation en assembleur.

Un contrôleur de disquettes peut vous rendre de très grands services. On en trouve dans le domaine public toute une série.

❐ 5.4.2. Désassembleur

Ce logiciel peut vous aider à effectuer un examen approfondi de vos programmes. Il se charge d'établir automatiquement le lien entre les chaînes numériques et les mnémoniques correspondants en langage machine, vous évitant ainsi de le faire à la main.

Ce logiciel permet en outre de reconvertir un boot-secteur enregistré dans un fichier à l'aide de VIRtuel T1.prg, en code source, et d'affecter des étiquettes.La reconversion du code machine en code assembleur est également réalisée par les programmes Profimat ou GFA-Assembleur.

❐ 5.4.3. Programmes antivirus

Nombreuses sont les revues spécialisées qui, depuis un certain temps, ont publié les codes de certains antivirus. Avec un peu d'expérience dans la programmation et un certain sens de déduction pour interpréter des listings parfois incorrects et incomplets, il est tout à fait possible de concevoir son propre anti-virus avec les variantes les plus diverses.

Certains programmeurs se sont employés à mettre cette possibilité en pratique et ont proposé leurs créations aux clubs du domaine public. Mais parmi eux, il y a également un certain nombre de programmeurs moins versés dans l'art de copier et de corriger les

erreurs ou même d'utiliser le système ; il faudra donc consacrer beaucoup de temps pour faire le tri dans tous ces programmes.

Etant donné que les programmes anti-virus sont distribués en règle générale sur des disquettes personnalisées, il faut parfois investir une certaine somme d'argent pour comparer, si possible, toutes les disquettes.

Chapitre 6

L'évolution du droit positif français

❐ 6.1. La nécessité de disposer de moyens de lutte légaux

Les juristes français ont pris conscience de la nécessité de disposer d'armes juridiques à la suite d'un double constat :

D'une part, celui du développement rapide de cette nouvelle technologie qu'est l'informatique, d'autre part celui de l'apparition corrélative d'une nouvelle criminalité, au rang de laquelle figure en bonne place l'introduction frauduleuse des virus.

❐ 6.2. La généralisation de l'informatique et le sentiment de vulnérabilité qu'elle provoque

Il ne fait aucun doute que l'informatique est entrée aujourd'hui dans une phase de grande diffusion, l'ordinateur étant maintenant présent dans tous les domaines d'activité, phénomène dont le juriste n'a pu faire abstraction.

Si le taux d'informatisation est bien entendu extrêmement variable selon les secteurs, son examen révèle que c'est évidemment dans les domaines de l'industrie et des services que la pénétration est la plus importante, domaines particulièrement sensibles en raison de l'importance qu'ils représentent dans l'économie d'une nation.

La possibilité de centraliser des données, l'extension des réseaux et la vitesse de circulation des informations, illustrations du développement de la technique informatique, s'ils traduisent un progrès technique considérable, n'en constituent pas moins une menace pour ceux qui l'utilisent, et en particulier pour l'individu.

S'il n'est certes pas facile de mesurer avec exactitude l'importance de ce phénomène, il n'en reste pas moins préoccupant.

L'état de dépendance dans lequel se trouvent notamment les entreprises vis-à-vis de leur système, rend la moindre défectuosité très lourde de conséquences.

Si des pannes ou des dysfonctionnements momentanés semblent inéluctables, il en va autrement de la fraude informatique, c'est-à-dire des comportements délictueux ayant pour objet ou pour moyen l'ordinateur.

Les enjeux de la sécurité informatique apparaissant considérables, la nécessité d'une réplique juridique qui définisse les modalités de la réaction sociale, s'est rapidement imposée.

Cette nécessité s'est fait d'autant plus cruellement sentir qu'était concomitamment constatée l'existence d'une véritable délinquance informatique.

❒ 6.3. L'apparition de la criminalité informatique

L'acte illicite que le juriste a cherché à appréhender peut se définir comme "tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de transmission de données.

S'il est difficile d'établir une typologie des actes répréhensibles ainsi que de ceux qui en sont les auteurs, on peut néanmoins tenter de décrire les quelques catégories dans lesquelles ils s'inscrivent.

Dans le même esprit, il parait possible de définir un profil type du délinquant et d'évaluer le coût des sinistres ainsi provoqués.

❐ 6.4. Typologie des actes frauduleux

La plupart des auteurs s'accordent pour distinguer 3 grandes catégories de délits au regard de la place qu'occupe l'informatique dans la structure concrète de l'acte délictueux.

1) *Cas dans lesquels l'informatique est l'objet même de la délinquance*

L'informatique est l'objet même de la délinquance en cas de sabotage d'ordinateur ou de vol de temps machine.

Le sabotage d'ordinateur est le plus souvent le fait de personnes ayant appartenu à l'entreprise qui en est victime.

Il s'agit en général davantage d'employés aigris, motivés par une vengeance personnelle qu'ils cherchent à assouvir, que de véritables criminels.

La forme la plus pernicieuse de cette délinquance consiste bien évidemment, par altération ou modification de programmes, à insérer dans les systèmes de véritables bombes logiques dont l'objet est au moyen d'un virus la destruction progressive des données ou des traitements.

Le vol de temps, certes moins porteur de danger, est également la plupart du temps réalisé par des salariés de l'entreprise considérée, qui utilisent pour une tâche qui leur est personnelle , l'outil mis à leur disposition dans le cadre de leur travail.

2) *Cas dans lesquels l'informatique est l'instrument de la fraude*

Cette hypothèse recouvre dans une large mesure les infractions contre la propriété et constitue ce que l'on pourrait appeler la criminalité économique commise à l'aide de l'ordinateur.

Au premier rang de ces actes répréhensibles, figurent toutes les manipulations informatiques, telles que les

modifications de salaires, les manipulations de positions bancaires, ou encore l'effacement de créances.

Dans cette même catégorie, on trouve l'ensemble des actes parfois commis par les porteurs de cartes bancaires, dont l'objet consiste à utiliser les failles des dispositifs techniques actuels, aux seules fins de se procurer indûment des espèces.

L'utilisation de l'informatique peut encore être un moyen de fraude dans certains cas d'espionnage dans lesquels on a recours à cette dernière comme moyen de se procurer une information en principe couverte par le secret.

Cette activité d'espionnage peut être entreprise tout aussi bien par une entreprise désireuse de percer le secret de son concurrent direct que par un état déterminé à se procurer des informations d'intérêt national.

C'est par l'introduction de virus dans les systèmes informatiques que les auteurs desdits actes parviendront à leurs fins.

Lorsque des particuliers sont directement victimes de telles manoeuvres, l'informatique est alors utilisée pour porter atteinte à la vie privée et à la confidentialité qui s'y attache.

On notera que la loi Informatique, Fichiers et Libertés, a été précisément élaborée pour tenter de sauvegarder l'individu contre de telles atteintes.

3) *Cas dans lesquels l'informatique fournit l'occasion du délit*

Dans cette dernière hypothèse, le lien avec l'informatique est cette fois beaucoup plus ténu, cette dernière étant seulement l'occasion des délits.

Ces derniers peuvent se manifester tant lors de la commercialisation des produits informatiques, que de leur utilisation.

la commercialisation d'un produit peut être l'occasion d'infractions pénales de droit commun telles que la contrefaçon, ou la publicité mensongère, ou encore être vecteur de la propagation de virus.

❒ 6.5. Typologie des délinquants

Il est assez difficile de dresser une typologie des délinquants, en raison notamment du fait qu'il est rare que les cas de criminalité informatique soient connus des autorités judiciaires ou fassent l'objet de publicité.

A la difficulté de détecter les crimes informatiques, s'ajoute le manque d'intérêt qu'ils suscitent de la part du public, et parfois même des dirigeants des entreprises qui en sont victimes.
Ces éléments ne sont pas de nature à faciliter l'élaboration d'un profil type des délinquants.

Toutefois, on peut estimer que le délinquant appartient en général à l'une des 4 catégories ci-après définies :

- Le jeune joueur ou le passionné d'informatique, animé par la seule curiosité technique et non par l'esprit de lucre.

  En général, ce dernier se contente de jouer les "voyeurs" dans les systèmes qu'il pénètre, survolant sans les modifier ni les détruire les données qui y sont contenues.

- L'informaticien qui volera un programme dans le but de le négocier ensuite auprès d'un tiers ou d'en tirer profit sous quelle que forme que ce soit.

- Le criminel de l'informatique, qui commettra sciemment et en toute connaissance de cause des actes de vandalisme.

- L'espion, agissant au bénéfice d'un concurrent ou d'un état, qui s'introduira dans un système .

  Il est généralement le mieux armé pour accomplir les actes

délictueux qu'il projette, et sera donc le plus difficile à retrouver et à appréhender.

En l'état actuel des informations dont on peut disposer, les enquêtes révèlent que parmi les auteurs identifiés on trouve le plus fréquemment des membres ou d'anciens membres de la structure directement victime de la fraude.

Ce sont ces deux dernières catégories, de loin les plus dangereuses, auxquelles nous consacrerons plus particulièrement notre étude.

❐ 6.6. Coût des sinistres

Si une large unanimité s'est dégagée pour estimer que la criminalité informatique est source de préjudices considérables, il n'en reste pas moins que nous disposons de très peu de chiffres nous permettant de définir avec exactitude le quantum des pertes qu'elle engendre.

La seule certitude que l'on possède en cette matière concerne l'accroissement des pertes occasionnées par la fraude d'une année à l'autre.

A cet égard, les estimations les plus raisonnables avancent un doublement annuel du coût de cette délinquance.

Une étude réalisée par la Police Judiciaire a permis de montrer que le montant moyen du préjudice financier subi s'élève à 2,2 Millions de francs et que pour l'année 1986 il a été recensé autant de délits que sur la période antérieure 1981-1985.

En 1984 des études américaines ont évalué le coût global de la fraude à 100 Millions de Dollars pour ce seul pays.

Si les données dont on dispose demeurent encore assez imprécises, il n'en est pas moins certain que les intérêts en jeu sont considérables et que la fraude informatique connaît un développement prodigieux, qui légitime les plus vives inquiétudes.

L'apparition de cette criminalité particulière et le constat de la généralisation de l'informatique ont contraint les juristes à

s'interroger sur les moyens à mettre en oeuvre pour réprimer cette nouvelle et dangereuse forme de délinquance.

❒ 6.7. La problématique juridique

La répression de l'introduction et de la propagation des virus a rencontré 2 principaux obstacles qui tiennent, d'une part à la nécessité de prendre en compte le caractère incorporel de l'objet à protéger, d'autre part aux difficultés rencontrées pour créér un véritable droit pénal de l'informatique.

La difficile appréhension juridique des biens informationnels

L'objet de la criminalité informatique est pour l'essentiel l'information contenue dans les systèmes, et donc un bien incorporel.

Le statut de l'information et son insertion dans notre ordre juridique français est d'ailleurs extrêmement controversé, et fait actuellement l'objet de vifs débats en doctrine.

C'est le seul constat de la valeur croissante des biens incorporels et de la place prépondérante qu'ils commencent à occuper dans l'économie, qui a conduit à certaines transformations, d'ailleurs encore très limitées dans leur portée.

L'examen du droit positif révèle que malgré quelques hésitations jurisprudentielles, appuyées par un certain nombre d'initiatives doctrinales, il est rare que l'acte illicite soit retenu en cas de manipulation de l'information seule, indépendamment de son support.

Cette difficulté s'est à plusieurs reprises manifestée pendant les débats parlementaires qui ont présidé à l'adoption de la loi du 5 Janvier 1988, dite loi sur la "Fraude Informatique".

Nous constaterons à cet égard, que cette dernière n'a pas pour objet de protéger les informations contenues dans les systèmes, mais bien davantage de réprimer l'accès frauduleux à ces informations.

Toutefois, la nécessité de disposer de moyens de répression à même d'endiguer le phénomène de la fraude est apparue plus importante que la résolution de cette difficulté juridique.

La difficile génèse d'un droit pénal de l'informatique.

Outre le problème précité, un autre obstacle est venu freiner l'appréhension par le droit pénal français de la criminalité informatique.

Il était, en effet, évident que seule une véritable politique pénale, jouant un rôle dissuasif au regard des risques qu'elle ferait encourir aux créateurs et propagateurs de virus pourrait se révéler efficace.

Néanmoins, bon nombre de pénalistes se déclaraient hostiles à ce qu'ils qualifient de "recours systématique au droit pénal".

En effet, ils considéraient que le recours au législateur n'aurait eu d'autre effet que de provoquer l'apparition de nouvelles infractions venant grossir le flot de la multitude de textes déjà existant.

Monsieur GODFRAIN, Député Français, Auteur de la proposition de loi sur la Fraude Informatique a tenté de sortir de cette spirale infernale en proposant d'insérer la répression de la fraude informatique, certes dans le code pénal, mais dans le cadre d'infractions préexistantes .

Ainsi que nous le constaterons, cette démarche n'était pas sans danger, en ce qu'elle mettait notamment en péril les définitions devenues classiques de certaines infractions, au risque de générer de nouvelles incertitudes dans d'autres domaines que celui de l'informatique.

C'est une des raisons pour lesquelles cette solution n'a pas été retenue dans le texte définitif.

En revanche, la voie de la création d'incriminations nouvelles est apparue préférable, en dépit des inconvénients qu'elle présente, notamment de l'inflation de textes pénaux à l'origine de laquelle elle se trouve.

C'était au demeurant la seule voie possible pour sanctionner efficacement l'introduction des virus.

❐ 6.8. L'insuffisance du droit pénal traditionnel

Les textes législatifs dont disposait la France comprenaient d'une part les quelques textes spécifiques à l'informatique, d'autre part les dispositions générales du droit pénal classique.

Leur examen ne manquera pas de révéler leur insuffisance et de nous faire prendre conscience de la nécessité qu'il y avait à voir le législateur intervenir en ce domaine particulier.

La législation spécifique à l'informatique

La Loi du 6 Janvier 1978

Ce texte contient des dispositions pénales relatives à l'informatique ; les délits et contraventions qu'il vise sont en substance les suivants :

- Absence de déclaration en cas de traitement d'informations nominatives par l'organisme qui gère les fichiers: 6 mois à 3 ans de prison et/ou 2000 à 200.000 Frs d'amende.
- Collecte et conservation illicites d'informations nominatives, suivant les moyens employés :

  1 à 5 ans de prison et/ou 20.000 à 200.000 Frs d'amende

- Divulgation d'informations nominatives :

  2 à 6 mois de prison ou 2000 à 20.000 Frs d'amende.

- Détournement de finalité :

  1 à 5 ans de prison et 20.000 à 2.000 000 Frs d'amende.

- Entrave à l'action de la CNIL, obstacle au droit d'accès... :

  Contravention de 5ème classe.

Le champ d'application de ce texte se trouve limité restrictivement par la référence expresse qui y est faite à la notion d'information nominative, qui interdit d'appréhender l'ensemble des malversations susceptibles d'être commises, et notamment l'utilisation de virus.

La Loi du 3 Juillet 1985

La Loi du 3 Juillet 1985 est venue consacrer la protection du logiciel au titre du droit d'auteur.

Les articles 425 et suivants du code pénal lui sont donc applicables.

Il en résulte donc que constitue une contrefaçon la reproduction d'un logiciel sans autorisation de l'auteur, quel que soit le logiciel et quel que soit le support, et ce même s'il s'agit d'une copie réservée à l'usage privé du copiste.

Constitue également une contrefaçon l'adaptation ou l'élaboration d'un programme dérivé sans l'accord de l'auteur.

Constitue encore une contrefaçon l'utilisation non autorisée d'un programme ou le débit, l'importation, l'exportation, la division, la diffusion d'un logiciel contrefait.

La sanction est une amende de 6000 à 120.000 Frs et/ou une peine de prison de 3 mois à 2 ans.

Ladite peine est doublée en cas de récidive et le Tribunal peut prononcer la fermeture de l'établissement exploité pour une durée pouvant aller jusqu'à 5 ans.

Si ces textes constituent incontestablement un outil efficace de lutte contre la contrefaçon et sans doute aussi un moyen détourné de réprimer la propagation des virus, il n'en demeure pas moins qu'ils ne sont pas d'une portée suffisante pour constituer l'arme absolue contre ces derniers, si tant est qu'il en existe une.

Il s'agit, en effet, de dispositions pénales insérées dans des lois spéciales pour sanctionner telle ou telle violation de leurs dispositions substantielles, ce qui en limite considérablement le champ d'application.

Dans ces conditions, on s'est alors interrogé sur la capacité d'adaptation à la délinquance informatique du droit pénal traditionnel des infractions contre les biens, notamment des incriminations de vol, escroquerie et abus de confiance.

Les dispositions pénales françaises de droit commun

1) *Les délits d'accès non autorisé à l'information*

La captation sans droit de données ou de programmes constitue sans nul doute le premier acte constitutif de la criminalité informatique qu'il est nécessaire de pouvoir appréhender.

Cette dernière peut se réaliser de diverses manières, selon qu'il y a ou non appréhension du support matériel des données.

La main mise sans droit sur le support matériel

Cette première hypothèse, qui est d'ailleurs loin d'être la plus fréquente, peut être parfaitement appréhendée par le droit pénal classique, par le biais du vol ou de l'abus de confiance.

Le vol est défini par l'article 379 du Code Pénal français qui dispose que "quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol".

En conséquence, la saisine sans droit du support de l'information permet incontestablement de caractériser le délit de vol.

S'il y a détournement du support alors que ce dernier avait été remis à l'occasion de l'un des contrats visés dans les textes réprimant l'abus de confiance, c'est à l'évidence cette dernière qualification qu'il conviendra de retenir.

Rappelons qu'en matière d'abus de confiance est puni d'emprisonnement "quiconque aura détourné ou dissipé au préjudice des propriétaires, possesseurs ou détenteurs, des effets, deniers, marchandises, billets, quittances ou tous autres écrits contenant ou opérant obligation ou décharge qui ne lui auraient été remis qu'à titre de louage, de dépôt, de mandat, de nantissement, de prêt à usage, ou pour un travail salarié ou non, à la charge de

le rendre ou représenter ou d'en faire un usage ou un emploi déterminé".

Le droit pénal classique est sans doute encore à même de sanctionner l'acte illicite lorsque il y a appréhension limitée du support, c'est à dire emprunt de ce dernier, puis restitution après duplication des données ou des programmes.

On sait en effet qu'une partie de la jurisprudence estime qu'il peut y avoir vol lorsque s'est révélée l'intention du fraudeur de se comporter en propriétaire, ne serait-ce que l'espace d'un temps.

La Cour de Cassation a d'ailleurs fait application de ce principe dans une espèce où un salarié avait photocopié des documents appartenant à son employeur à des fins personnelles.

Elle décide qu'il y a vol dès lors que le document a été soustrait indûment le temps d'effectuer la photocopie, quand bien même est-il restitué immédiatement après.

On peut dès lors peut-être estimer, encore qu'aucune décision ne le confirme à ce jour, que cette solution pourrait être appliquée à celui qui procède à la duplication sur un support de données figurant sur un autre support auquel il a eu accès.

On remarquera que d'autres incriminations pourraient venir s'adjoindre à celle de vol, lorsque la manipulation en cause suppose l'usage d'un faux nom ou d'un code.

En particulier, on peut considérer qu'il sera alors possible de retenir le délit d'escroquerie, l'usage du code constituant les manoeuvres frauduleuses indispensables pour caractériser celui-ci.

Si le droit commun peut donc dans ce cas se révéler utile, on ne pouvait néanmoins s'en satisfaire dans la mesure ou la notion même de virus est la plupart du temps antinomique de celle d'appréhension du support.

L'entrée sans droit dans un système

La situation est déjà beaucoup moins claire dans le domaine du vol de temps machine, qui constitue pourtant une des activités illicites les plus répandues.

Dans cette hypothèse, il est bien certain qu'on se trouve en présence d'une utilisation, certes passagère, mais néanmoins abusive, de la propriété d'autrui.

Compte tenu du particularisme de "l'objet" volé, qui se caractérise essentiellement par sa fluidité, la qualification pénale à retenir pour appréhender le phénomène pose de sérieuses difficultés.

Par analogie avec le vol d'électricité, dont la jurisprudence française a fait application a de multiples reprises, la majeure partie des auteurs s'accordent à reconnaître que cette qualification devrait s'appliquer.

Néanmoins, d'autres se montrent plus favorables à l'escroquerie.

L'insuffisance du droit pénal commun apparaît encore plus évidente à propos de la simple captation d'informations à distance, qui se réalise précisément grâce au virus.

Un examen de la doctrine révèle que cette dernière soutient parfois qu'une information seule peut donner lieu à un vol, un recel, une escroquerie ou un abus de confiance, du moins lorsque l'appropriation frauduleuse est accompagnée ou suivie d'une activité matérielle opérant transfert de l'information d'un patrimoine vers un autre.

Si séduisante que cette thèse puisse paraître, elle ne paraît cependant pas refléter l'état du droit positif.

L'examen des conditions auxquelles doit satisfaire un délit pour être qualifié de vol en France nous en fournira une illustration.

En premier lieu, le vol suppose que puisse être caractérisé un acte d'appréhension, de soustraction, sur un objet matériel se trouvant en possession de la victime.

Cette soustraction paraît difficile à caractériser en matière de bien informationnel.

En effet, en ce domaine il ne peut y avoir déplacement de la chose, mais simplement dédoublement.

Il semble délicat de parler de déplacement de la chose, même si l'on admet que lorsque l'emprunt s'effectue par l'intermédiaire des réseaux, on peut suivre fictivement l'information tout au long de son trajet.

Si l'emprunt se réalise de manière plus subtile, par l'utilisation des voies hertziennes notamment, alors cette thèse apparaît inapplicable.

Seul le concept selon lequel toute appréhension de valeur caractériserait la soustraction, permettrait de surmonter la difficulté.

Cependant, force est de constater qu'aucune illustration de celui-ci ne peut être trouvée en jurisprudence.

En second lieu, caractériser le vol suppose que l'objet du délit soit une chose susceptible d'appropriation.

Or, il n'est pas certain que le bien informationnel puisse en faire l'objet, notamment en ce qu'il n'est pas mesurable et en ce qu'il demeure conservé par la victime.

Dans ces conditions, on peut hésiter à voir dans l'information une chose susceptible d'être soustraite et donc de faire l'objet d'un vol.

Les incertitudes juridiques auxquelles donne lieu la volonté de répression permettent à l'évidence de conclure à l'insuffisance du droit pénal classique en ce domaine particulier.

2) *Les délits emportant l'altération ou la destruction de données ou de systèmes informatisés*

Dans le cas de figure dans lequel nous nous plaçons, il s'agit en réalité d'appréhender les atteintes à l'intégrité de l'information

susceptibles de se réaliser par voie de destruction ou de trucage des données, et donc par l'introduction de virus.

Il est parfaitement évident qu'une information peut se trouver privée de toute valeur si elle est totalement ou partiellement effacée ou altérée.
Il n'existe pas dans notre droit pénal traditionnel de dispositions particulières.

La question s'est donc posée de savoir si ces comportements pouvaient être appréhendés à l'aide des dispositions générales préexistantes.

En premier lieu, on peut songer à faire application des dispositions de l'article 434 du Code Pénal qui sanctionne "quiconque aura volontairement détruit ou détérioré un objet mobilier ou un bien immobilier appartenant à autrui".

Un examen de la doctrine autorise à penser que la portée de cette disposition dans notre domaine est singulièrement réduite.

Si ce texte permet de réprimer les destructions ou détériorations de l'ordinateur et ses périphériques, on peut en revanche douter de son applicabilité à l'altération des données par introduction de virus.

En effet, il semble difficile d'assimiler à un objet mobilier les informations contenues dans un système.

On pourrait certes songer, pour contourner la difficulté, à assimiler la détérioration à la destruction du support sur lequel se trouve l'information, l'intrusion provoquant en quelque sorte un changement de son état.

Mais il paraît pour le moins douteux qu'une telle analyse puisse être consacrée par la jurisprudence.

En second lieu, on s'est également interrogé sur l'éventualité de l'application de l'article 439 du Code Pénal qui punit "quiconque aura volontairement brûlé ou détruit d'une manière quelconque des registres, minutes ou actes originaux de l'autorité publique, des titres, billets, lettres de change, effets de commerce ou de banque,

contenant ou opérant obligation, disposition ou décharge; quiconque aura sciemment détruit, soustrait, recelé, dissimulé ou altĕré un document public ou privé de nature à faciliter la recherche des crimes et délits, la découverte des preuves ou le châtiment de leur auteur".

On s'est une fois de plus demandé si cet article était susceptible de recevoir application dans la mesure où l'informatique sert de plus en plus à mémoriser des données ayant une valeur probante.

Outre le fait qu'il convient de se trouver dans ce cas particulier, il semble bien que l'article 439 sous entend que sa mise en oeuvre ne pourra s'effectuer que dans le cas de destruction d'un écrit, ce qui le rend donc totalement inopérant dans l'hypothèse qui nous préoccupe.

Si l'on tente de faire appel à d'autres infractions, un examen détaillé de leurs éléments constitutifs révèle qu'en pratique leur mise en oeuvre est des plus problématique.

Il en est ainsi notamment des incriminations du faux en écriture ou de celles protégeant le secret.

Le faux en écriture fait l'objet de diverses incriminations dans notre code pénal.

En particulier, le faux en écriture privée, de commerce ou de banque est puni de peines d'emprisonnement.

La falsification peut constituer, soit dans l'altération de l'écrit, soit dans la déformation de l'information exprimée dans un écrit constituant un titre juridique.

A l'examen des textes, il apparaît que les informations visées sont supposées se trouver sur un support écrit, et il semble donc difficile de les transposer pour en faire application au cas qui nous préoccupe.

On ne saurait, en effet, oublier un principe fondamental de notre droit pénal, qui est celui de l'interprétation stricte des textes.

En conséquence, le raisonnement par analogie est prohibé.

Il en est de même des incriminations qui gouvernent le secret, l'obligation de confidentialité n'étant imposée que dans des cas particuliers qui tiennent, soit à la qualité de son détenteur, soit à la nature de l'information.

De cette brève analyse des textes de droit pénal classique applicables, on ne peut que conclure à leur insuffisance ou plutôt à leur inadaptation pour assurer une juste et efficace répression de la criminalité informatique dans sa forme la plus pernicieuse: le virus.

Même si les incriminations permettent d'appréhender certains comportements, il est manifeste qu'elles ne constituent pas le moyen de lutte attendu contre cette nouvelle forme de criminalité, une multitude de comportements délictueux échappant à leur sanction.

Une répression ne peut, en effet, se révéler efficace et dissuasive que si elle permet d'appréhender l'ensemble des comportements délictueux qu'elle vise à réprimer.

C'est à la suite de ce constat que Monsieur Jacques GODFRAIN, député de l'AVEYRON, a, au mois d'août 1986, déposé sur le bureau de l'Assemblée une proposition de loi qui s'est traduite par l'adoption d'un texte spécifique en Janvier 1988.

❐ 6.9. La proposition de loi Godfrain

La proposition de loi de Monsieur GODFRAIN se caractérisait avant tout par son caractère pragmatique, aucun à priori idéologique n'ayant influencé son analyse.

Elle résultait d'une double démarche, qui a consisté, d'une part à étendre le champ d'application d'infractions préexistantes pour y introduire expressément des procédés frauduleux liés à l'utilisation de l'informatique, d'autre part à définir de nouveaux délits.

On remarquera que cette proposition avait pour principal objet de protéger directement les informations contenues dans les systèmes, peut-être davantage que de réprimer l'accès frauduleux à ces informations.

❐ 6.10. L'élargissement des incriminations existantes

La proposition de loi offrait donc de compléter certains textes pénaux existant afin de permettre leur application au domaine particulier de la fraude informatique, et en particulier au virus.

On soulignera que cette démarche s'apparente à celle suivie par un certain nombre de législations étrangères.

L'escroquerie

L'article 5 de la proposition de loi visait à étendre à la criminalité informatique les dispositions du code pénal relatives à l'escroquerie.

Ainsi, l'usage indû d'un code d'identification ou d'accès "ayant pour but la remise de fonds, de meubles, d'obligations, dispositions, billets, promesses, quittances ou décharges, ou des programmes enregistrés ou la prise de faux noms ou de fausses qualités destinés à se faire remettre des données ou programmes" seraient qualifiés d'escroquerie et sanctionnés par l'article 405 du Code Pénal.

Le délit d'escroquerie est donc constitué, d'une part en cas d'usage indû d'un code d'accès ou d'identification, d'autre part en cas de manoeuvres destinées à se faire remettre ou délivrer des données ou programmes informatiques.

L'abus de confiance

L'article 6 de cette même proposition avait pour objet une modification des dispositions relatives à l'abus de confiance, dans le but de sanctionner celui qui aurait détourné les données ou programmes à lui remis à l'occasion des contrats prévus par le Code, tels que le louage, le dépôt, le mandat, le nantissement et le prêt à usage.

Une telle modification avait pour objet de permettre de retenir cette qualification sans discussion aucune, en particulier en cas de détournement de programmes ou données par un salarié.

L'auteur d'un tel détournement serait passible d'une peine de 2 mois à 2 ans d'emprisonnement et d'une amende allant jusqu'à 2,5 Millions de francs.

La dégradation et la destruction

Il était encore proposé par Monsieur GODFRAIN de modifier les dispositions du code qui répriment ceux qui détruisent ou détériorent volontairement des biens mobiliers ou immobiliers appartenant à autrui.

Si ces dispositions autorisent, en effet, l'incrimination des destructions d'ordinateurs, elles ne couvrent pas les agissements ayant pour effet, par l'introduction d'instructions erronées, de rendre inutilisables les logiciels et les informations contenues dans l'ordinateur.

La proposition de loi prévoyait en outre d'étendre la sanction à quiconque aurait volontairement détruit ou détérioré une donnée ou un programme enregistré.

De la même façon, il était prévu que l'article 439 du Code Pénal relatif à la destruction de preuves, ferait expressément référence à la criminalité informatique.

On remarquera à cet égard que cette incrimination suppose que soit démontré le caractère intentionnel de l'acte perpétré, ce qui pourrait soulever de sérieuses difficultés de preuve.

Outre l'extension d'incriminations préexistantes, la proposition de loi initiale donnait naissance à des incriminations nouvelles :

Annexe

❒ A.1. Tables

❒ A.1.1. Table de conversion décimale-héxadécimale

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
2	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
3	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
4	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
5	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
6	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
7	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
8	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
9	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
A	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
B	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
C	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
D	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
E	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
F	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

❐ A.1.2. Codes ASCII

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0		0		0	@	P	`	p	Ç	É	á	ã	ĳ	ס	α	≡
1	⇧	1	!	1	A	Q	a	q	ü	æ	í	õ	Ĳ	ע	β	±
2	⇩	2	"	2	B	R	b	r	é	Æ	ó	Ø	א	פ	Γ	≥
3	⇨	3	#	3	C	S	c	s	â	ô	ú	ø	ב	צ	π	≤
4	⇦	4	$	4	D	T	d	t	ä	ö	ñ	œ	ג	ק	Σ	⌠
5	☒	5	%	5	E	U	e	u	à	ò	Ñ	Œ	ד	ר	σ	⌡
6	◢	6	&	6	F	V	f	v	å	û	ª	À	ה	ש	µ	÷
7	▣	7	'	7	G	W	g	w	ç	ù	º	Ã	ו	ת	τ	≈
8	✓	8	(	8	H	X	h	x	ê	ÿ	¿	Õ	ז	ן	Φ	°
9	🕒	9	)	9	I	Y	i	y	ë	Ö	⌐	¨	ח	ך	Θ	•
A	🔔	ə	*	:	J	Z	j	z	è	Ü	¬	´	ט	ם	Ω	·
B	♪	ESC	+	;	K	[	k	{	ï	¢	½	†	י	ף	δ	√
C	FF	[illegible]	,	<	L	\	l	|	î	£	¼	¶	כ	ץ	∮	ⁿ
D	CR	[illegible]	-	=	M	]	m	}	ì	¥	¡	©	ל	§	φ	²
E	[illegible]	[illegible]	.	>	N	^	n	~	Ä	ß	«	®	מ	∧	∈	³
F	[illegible]	[illegible]	/	?	O	_	o	Δ	Å	ƒ	»	™	נ	∞	∩	¯

❒ A.1.3. Programmes et variables système

Nous allons vous présenter les principaux programmes qui modifient les variables système. Vous pouvez vous référer à cette liste chaque fois que VIRtuel T2.acc vous signale une modification dans les variables système. Nous n'avons pas précisé le contenu de ces variables car il varie selon les paramètres d'installation des programmes. Vous pouvez ajouter à cette liste tous les autres programmes dont nous n'avons pas fait mention.

Programme	Adresse des variables
Détective	$408
Dosshell	$404
AHDI	$472, $476, $47e
Ramdisk	$472, $476, $47e
DiskSpeeder	$472, $476, $47e
Hardcopys	$502

Pour vous aider à établir une classification approximative des programmes que nous n'avons pas mentionnés ici, voici les principales variables vérifiées par VIRtuel avec leur signification. Cette liste vous permettra d'identifier l'origine des modifications détectées par VIRtuel.

ETVTIM **400** Event-Time-Vector de GEM. Cette variable permet d'exécuter des tâches répétitives

ETVCRT **404** Critical Error Handler. Cette variable est appelée en cas d'erreur sur la disquette

ETVTRM **408** Event Term. Cette variable est appelée avant de quitter un programme

SEEKRT **440** Seek-Rate (le temps nécessaire aux têtes de lecture pour passer sur la piste suivante)

NVBLS **454** Nombre de routines d'interruption de la VBL

VBLQUE	**456**	Pointeur sur la liste de routines appelée lors d'une interruption de la VBL
HDINIT	**46a**	Initialisation des lecteurs
DHDBBPB	**472**	Récupération du bloc de paramètres BIOS
HDVRW	**476**	Routine de lecture/écriture
HDBOOT	**47a**	Chargement d'un bootsecteur
HDMEDI	**47e**	Routine de changement de support (Insérez une nouvelle disquette !)
DSKBUF	**4c6**	Pointeur sur la mémoire-tampon d'une disquette La taille de cette mémoire est de 1024 octets.
HRDCPY	**502**	Vecteur de copie d'écran

❐ A.2. Utilisation de Atari Desktop

Nous allons décrire brièvement les principales fonctions d'Atari que vous devez connaître avant d'aborder le programme VIRtuel.

❐ Lancer les programmes

Pour lancer un programme à partir de l'environnement Atari ST, vous pouvez procéder de deux façons différentes :

Première méthode

Amenez le pointeur de votre souris sur le symbole du programme désiré dans la fenêtre active et cliquez deux fois sur le bouton gauche.

Deuxième méthode

Avec la souris, pointez sur le symbole du programme désiré dans la fenêtre active et cliquez une seule fois sur le bouton gauche. Le symbole du programme est ainsi activé et apparaît en vidéo inversée. Cliquez maintenant sur l'option Ouvrir du menu Fichier.

Index

A

Annuler 4-104, 4-107
Archiver les boot-secteurs 4-109
Atari ST 4-59

B

Bacille du charbon 3-56
Bactéries 2-47
Boot-secteur 3-53
Boot-virus 2-39,4-68, 4-70, 5-123

C

Catégories de virus 2-37
Central System Infector Virus 2-38
Charger 4-65, 4-67
Chevaux de Troie 2-47
Classification des virus 2-37
Contrôleur de disquette 5-127

D

Décontamination 5-123
Définition des virus 1-32
Démarrer 4-66
Dépistage
. des boot-virus 4-70
. des link-virus 4-76
Désassembleur 5-127

Diagnostic 4-68, 4-70
Disque C, D... 4-69
Disque(tte) 4-68

E

Ecrire 4-67
Enlever 4-67
Etablir un diagnostic 4-80

F

FAT 2-48
Fin 4-66
Format des fichiers 4-116

G

General Purpose Infector Virus 2-37

H

Historique 1-23

I

Insérer 4-67
Installation de VIRtuel 4-62

L

Link-virus 2-39, 3-56, 4-68, 4-70, 5-126
Lire 4-67
Liste de logiciels 4-91

M

Manipulation virale 1-22

Menu
. Atari 4-64
. Editer 4-66
. Fichiers 4-65
. Tester 4-68
Messages
. d'avertissement 4-87, 4-103
. d'erreurs 4-114
MicroVirus 3-52
Modification de vecteurs 4-106

N

Nouveau 4-65

O

Outils de diagnostic 5-126

P

Programmes antivirus 5-127

R

RAZ Système 4-66
Renommer 4-104, 4-106

S

Sauver 4-66, 4-68, 4-104, 4-107
Sauver avec nom 4-66
Special Purpose Infector Virus 2-37
Symptômes 1-22

T

T1.prg 4-62
T2.acc 4-63
TOS 4-59

V

Variables système 4-106
Vérification
. automatique 4-90
. manuelle 4-69
Vers 2-48
Very Clever General Purpose Infector Virus 2-37
VIRtuel 4-59
Virus 1-15
. Aladin 3-52
. batch 2-46
. évolutifs 2-46
. résidents en mémoire 2-44
. VCS 3-57

Dans la même collection...

Référence	Titre		Prix T.T.C.
...			
ML156	Bien débuter avec l'ATARI ST et STe		129.00
ML527	Bien débuter en GFA BASIC 2.0 et 3.0		129.00
ML561	Bien débuter Le Rédacteur		129.00
ML631	Boîte à Outils ST	disquette incluse	299.00
ML688	Dév. s/SUPERBASE PRO/PROIII	disquette incluse	299.00
ML172	Disquette et Disque Dur		179.00
ML272	Disquette et Disque Dur	disquette incluse	279.00
GL102S	Guide SOS GFA BASIC 2.0 à 3.0		99.00
ML530	Le Grand Livre de l'ATARI ST		199.00
ML530 OS	Pack Le Grand Livre de l'ATARI ST +Additif + freeware		199.00
ML556	Le livre de CALAMUS		199.00
ML573	Le livre de SUPERBASE (versions II, PRO, PRO III)		169.00
ML550	Le livre du Développeur sur ATARI ST		299.00
ML589	Le livre du Développeur sur ATARI ST (T2)		199.00
ML689	Le livre du Dév. sur ATARI ST (T2)	2 disquettes incluses	299.00
ML502	Le livre du Graphisme		199.00
ML602	Le livre du Graphisme	2 disquettes incluses	299.00
ML141	Le livre du Langage Machine		149.00
ML193	Le livre de l'intelligence Artificielle		179.00
ML616	Le livre de 1ST WORD PLUS	disquette incluse	299.00
ML185	Le livre du GFA BASIC 2.0		199.00
ML285	Le livre du GFA BASIC 2.0	disquette incluse	299.00
ML571	Le livre du GFA BASIC 3.0		199.00
ML671	Le livre du GFA BASIC 3.0	disquette incluse	299.00
ML299	Trucs et Astuces en GFA 2.0	disquette incluse	269.00
ML651	Trucs et Astuces ATARI ST	disquette incluse	299.00
...			

Achevé d'imprimer
sur les presses de l'imprimerie IBP
à Rungis (Val-de-Marne 94) (1) 46.86.73.54
Dépôt légal - Janvier 1990
N° d'impression: 5199



LE LIVRE ET
LE LOGICIEL

LE PACK ANTIVIRUS

U. GOHLKE

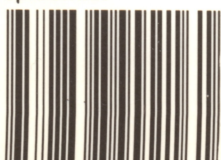
LE PACK ANTIVIRUS : un puissant logiciel de protection, mais aussi un ouvrage pratique pour travailler en toute tranquillité avec votre Atari.

LE LIVRE. Quels sont les symptômes d'une infection?... Que faire pour sauver ses programmes d'une destruction irréversible?... Ce livre explique le comportement, les mécanismes d'action et de reproduction des virus. Des informations pratiques vous permettront d'acquérir les réflexes élémentaires de protection :

- Les virus les plus répandus : Aladin, virus VCS, Key virus...
- Les mesures de prévention.
- La décontamination des programmes déjà atteints.
- Les programmes de détection du domaine public, etc...

LE LOGICIEL "VIRTUEL". Disposez d'un programme capable de détecter tout virus infiltré sur une disquette. Ce logiciel en analyse les boot-secteurs, mémorise ceux reconnus comme inoffensifs, signale les cas suspects, et vérifie enfin toute modification intervenue dans les fichiers programme. Ses caractéristiques techniques :

- Contrôle de tous les programmes, overlays et accessoires.
- Différents algorithmes de contrôle.
- Sauvegarde des boot-secteurs originaux pour un traitement ultérieur.
- Contrôle automatique de 1 à 30 programmes et de tous les pointeurs importants du système pour prévenir les risques d'épidémie.



Réf. ML 657. Prix 199 F
ISBN : 2-86899-216-1 / ISSN : 0980-1928
EDITIONS MICRO APPLICATION
58, RUE DU FAUBOURG POISSONNIÈRE
75010 PARIS. TÉL. : (1) 47 70 32 44